IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

MARGUERITE KUROWSKI and BRENDA MCCLENDON, on behalf of themselves and all others similarly situated, *Plaintiffs*, v. RUSH SYSTEM FOR HEALTH d/b/a RUSH UNIVERSITY SYSTEM FOR HEALTH, *Defendant*.	Case No. 22 Civ. 5380 (MFK) **JURY TRIAL DEMANDED**

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Marguerite Kurowski ("Kurowski") and Brenda McClendon ("McClendon") (collectively "Plaintiffs"), on behalf of themselves and all others similarly situated, upon personal knowledge as to Plaintiffs' own conduct and on information and belief as to all other matters based upon investigation of counsel, such that each allegation has evidentiary support or is likely to have evidentiary support upon further investigation and discovery, and for their Class Action Complaint against Defendant Rush System for Health d/b/a Rush University System for Health ("Rush" or "Defendant"), state as follows:

NATURE OF THE ACTION

1. Medical providers have a duty to patients to keep patient data, communications, diagnoses, and treatment information completely confidential unless authorized to make disclosures by the patient.

2. Patients are aware of and must be able to rely upon the protections, obligations, and expectations provided by statutory, regulatory, and common law as well as the promises of confidentiality contained within the Hippocratic Oath.

3. A patient who exchanges communications with Rush has a reasonable expectation of privacy that their personally identifiable data and the content of their communications will not be intercepted, transmitted, re-directed, or disclosed by Rush to third parties without the patient's knowledge, consent, action or authorization.

4. Rush nonetheless discloses Plaintiffs' and Class members' personally identifiable patient data, including their status as patients and the contents of their communications with Rush, to third parties including Facebook,[1] Google, and a digital advertising company called "Bidtellect."

5. Despite its ethical and legal obligations and its patients' reasonable expectations of privacy, Rush systematically violated and continues to violate the medical privacy rights of its patients by causing the contemporaneous unauthorized interception and transmission of personally identifiable patient data, and re-direction and disclosure of the precise content of patient communications with Rush to third parties including Facebook, Google, and Bidtellect without patient knowledge, consent, authorization, or any affirmative action.

6. Rush's conduct gives rise to at least eleven causes of action: (1) violation of § 2511 of the ECPA; (2) breach of the implied duty of confidentiality; (3) violations of the Illinois

[1] All allegations related to data transmissions to Facebook and Google are made as of the date of the initial Complaint (Dkt. 1), September 30, 2022. Plaintiffs' investigation revealed the undisclosed transmissions to Facebook and Google that were alleged in the initial Complaint. It appears that the source code for Rush's web properties was changed sometime in or around late March 2023, Google transmissions from within MyChart seem to have ceased, and Facebook transmissions have ceased altogether from both MyChart and www.rush.edu. To be clear, as of the date of this filing, data transmissions alleged as to Bidtellect, and transmissions to Google from communications with patients at www.rush.edu still appear to be ongoing.

Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq*.; (4) violations of the Illinois Deceptive Trade Practices Act, 815 ILCS 510/1 *et seq*; (5) invasion of privacy - intrusion upon seclusion; (6) invasion of privacy – public disclosure of private facts; (7) trespass to chattels; (8) breach of contract; (9) breach of the duty of good faith and fair dealing; (10) unjust enrichment; and (11) violation of the Illinois Eavesdropping Statute, 720 ILCS § 5/14-1, *et seq*.

7. As a result of Rush's conduct in disclosing personally identifiable patient data and re-directing and disclosing the content of patient communications to third parties without patient knowledge, consent, authorization, or any further action by the patient, Rush has caused damage to Plaintiffs and other patient Class members in that:

a. Sensitive and confidential information that Plaintiffs and patient Class members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the provider-patient relationship;

c. Defendant took something of value, to wit: personal data, from Plaintiffs and patient Class members and derived benefit therefrom without Plaintiffs and Class members' knowledge or informed consent or authorization and without sharing the benefit of such value;

d. Plaintiffs and other patient Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

e. Defendant's actions diminished the value of Plaintiffs and Class members' personal information.

PARTIES TO THE ACTION

8. Plaintiff Marguerite Kurowski is a resident of Will County, Illinois, a Rush patient, and MyChart patient portal user. Kurowski has been a Rush patient since approximately 2017 and has been a MyChart patient portal user since 2017.

9. Plaintiff Brenda McClendon is a resident of Cook County, Illinois, a Rush patient and MyChart patient portal user. McClendon has been a Rush patient since approximately 1999 and has been a MyChart patient portal user since 2017.

10. Defendant Rush System for Health d/b/a Rush University System for Health is an Illinois non-profit corporation headquartered in Chicago, Illinois. Rush encourages patients to use, and communicates with patients through the Rush web properties, including the MyChart patient portal. Rush University Medical Center, Rush Copley Medical Center, and Rush Oak Park Hospital are all part of Rush.

JURISDICTION AND VENUE

11. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332, because: (a) this is a proposed class action in which there are at least 100 Class members; (b) the parties are minimally diverse, as at least one member of the proposed patient Class is domiciled in a different state than Defendant; and (c) the combined claims of Class members exceed $5,000,000, exclusive of interest, attorneys' fees, and costs.

12. This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331 because the action arises under the laws of the United States, specifically, 18 U.S.C. § 2511, of the Electronic Communications Privacy Act ("ECPA").

13. This Court additionally has supplemental jurisdiction over Plaintiffs' state law claims under 28 U.S.C. § 1367(a), because they are so related to Plaintiffs' federal claims that they form part of the same case or controversy under Article III of the United States Constitution.

14. This Court has personal jurisdiction over Rush because Rush regularly conducts business throughout northern Illinois.

15. Venue is also appropriate in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this district.

FACTUAL ALLEGATIONS

I. RUSH PATIENTS HAVE REASONABLE EXPECTATIONS OF PRIVACY

16. Rush maintains various web properties, including www.rush.edu and mychart.rush.edu, for its patients to communicate with Rush, including but not limited to exchanging communications about bill payment, doctors, services, treatments, conditions, appointments, and access to an online MyChart patient portal.

17. Rush actively encourages patients to use its web properties, including the MyChart patient portal.

18. Plaintiffs are patients of Rush and users of the MyChart patient portal.

19. As Rush patients, Plaintiffs have a reasonable expectation of privacy that Rush, their health care provider, and its business associates, including Epic Software Systems, will not disclose their personally identifiable information or the content of their communications to third parties without their express authorization.

20. Plaintiffs' and other Rush patients' reasonable expectations of privacy in their personally identifiable data and communications exchanged with Rush are derived from several sources, including:

a. Rush's status as Plaintiffs' and other patients' health care provider;

b. Rush's common law obligation to maintain the confidentiality of patient data and communications;

c. State and federal laws and regulations protecting the confidentiality of medical information;

d. State and federal laws protecting the confidentiality of communications and computer data;

e. State laws protecting unauthorized use of personal means of identification;

f. Defendant's express promises of confidentiality; and

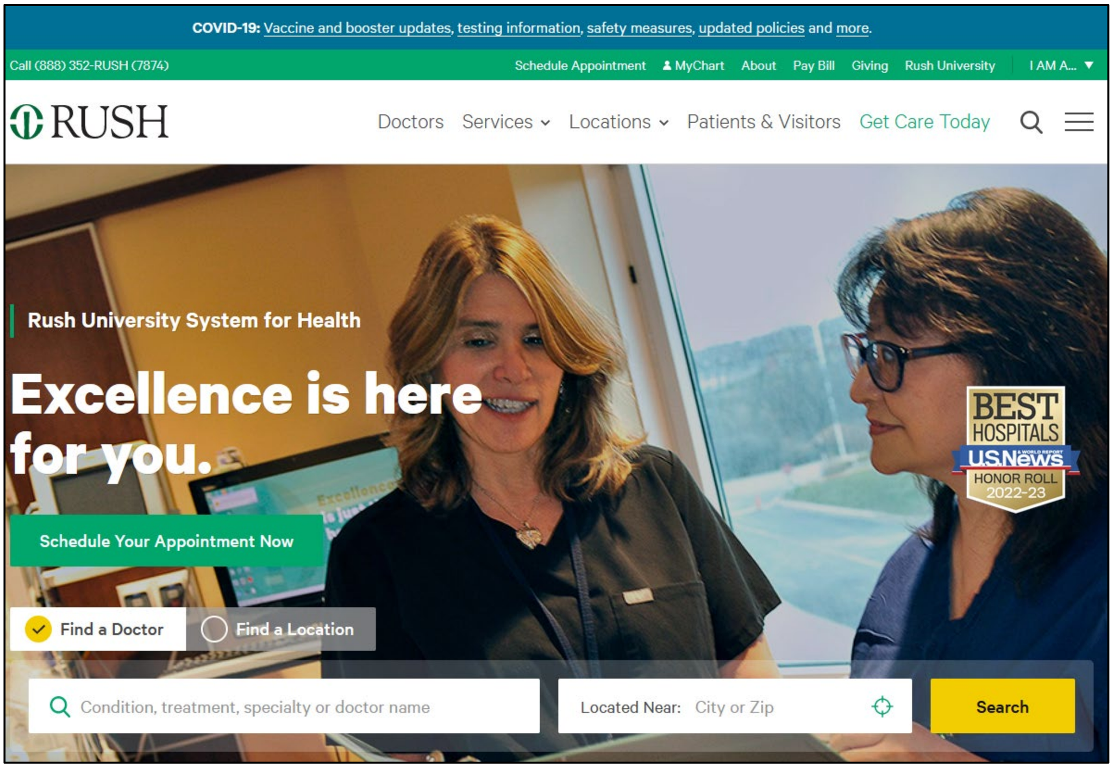
g. Defendant's implied promises of confidentiality.

II. THE RUSH WEB-PROPERTY

21. Plaintiffs interacted with Rush's web properties, including using the website to create an account on Rush's MyChart patient portal and log in to Rush's patient portal.

22. Plaintiffs exchanged communications with Rush via the Rush web properties, including using Rush's MyChart patient portal, identifying themselves to Rush as a patient, and exchanging communications relating to their particular providers and medical conditions.

23. Rush's homepage shows how the web property is designed for use by patients. The homepage provides patients with tools to "Find a Doctor," "Find a Location," search for "Condition, treatment, specialty or doctor name," "Schedule Appointment," Pay Bill," and access the "MyChart" patient portal:


COVID-19: Vaccine and booster updates, testing information, safety measures, updated policies and more.
Call (888) 352-RUSH (7874)
Schedule Appointment
MyChart
About
Pay Bill
Giving
Rush University
I AM A... ▼
RUSH
Doctors
Services
Locations
Patients & Visitors
Get Care Today
Rush University System for Health
Excellence is here for you.
Schedule Your Appointment Now
BEST HOSPITALS
U.S.News
HONOR ROLL 2022-23
✓ Find a Doctor
○ Find a Location
Condition, treatment, specialty or doctor name
Located Near: City or Zip
Search

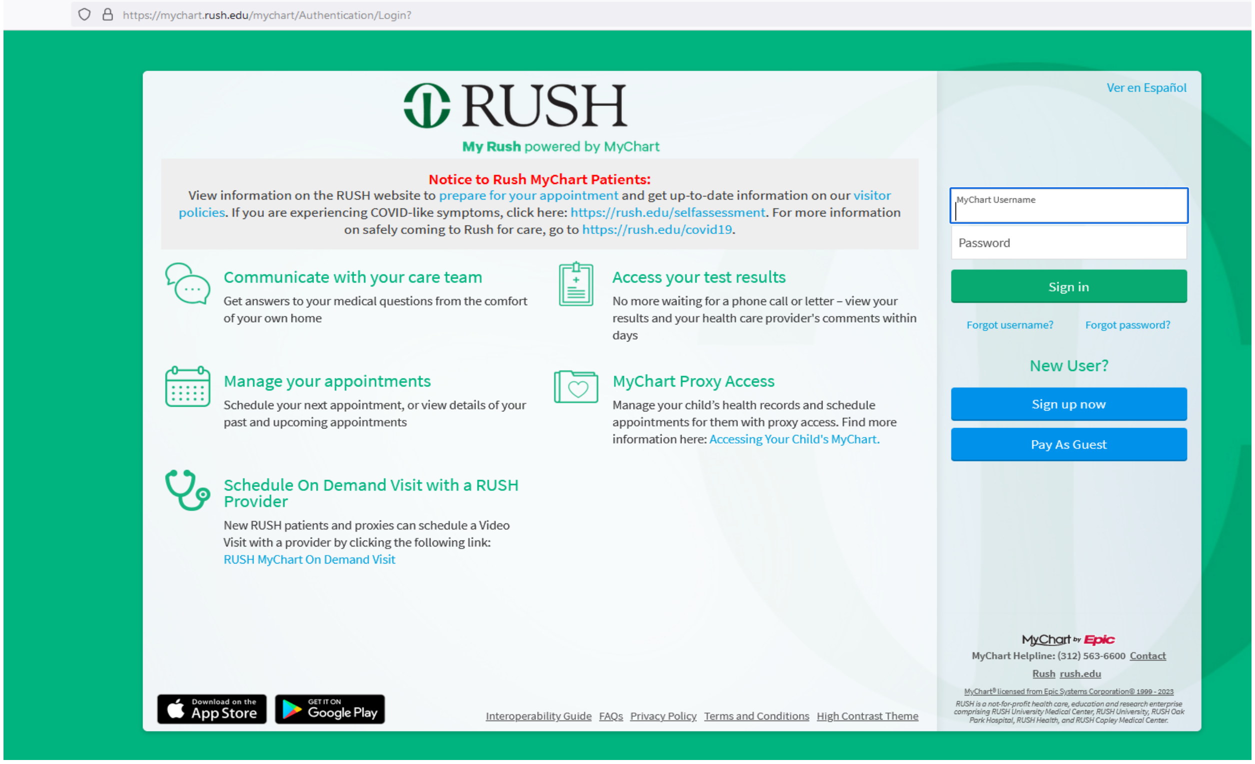
III. The MyChart Patient Portal

24. Rush also maintains a patient portal for its patients to communicate with Rush, with options including but not limited to "communicate with your care team," "access your test results," and "manage your appointments."

25. Rush maintains the web property at mychart.rush.edu as a login page for patients to log into Rush's MyChart patient portal.

26. Every Rush patient who logs into Rush's MyChart patient portal from Rush's website does so through the mychart.rush.edu login page.

27. Every Rush patient who logs into Rush's MyChart patient portal from Rush's website sees the mychart.rush.edu login page, which currently looks like this:



Notice to Rush MyChart Patients:
View information on the RUSH website to prepare for your appointment and get up-to-date information on our visitor policies. If you are experiencing COVID-like symptoms, click here: https://rush.edu/selfassessment. For more information on safely coming to Rush for care, go to https://rush.edu/covid19.

Communicate with your care team
Get answers to your medical questions from the comfort of your own home

Access your test results
No more waiting for a phone call or letter – view your results and your health care provider's comments within days

Manage your appointments
Schedule your next appointment, or view details of your past and upcoming appointments

MyChart Proxy Access
Manage your child's health records and schedule appointments for them with proxy access. Find more information here: Accessing Your Child's MyChart.

Schedule On Demand Visit with a RUSH Provider
New RUSH patients and proxies can schedule a Video Visit with a provider by clicking the following link: RUSH MyChart On Demand Visit

MyChart Helpline: (312) 563-6600 Contact Rush rush.edu

MyChart® licensed from Epic Systems Corporation© 1999 - 2023

RUSH is a not-for-profit health care, education and research enterprise comprising RUSH University Medical Center, RUSH University, RUSH Oak Park Hospital, RUSH Health, and RUSH Copley Medical Center.

https://mychart.rush.edu/mychart/Authentication/Login? (last visited March 21, 2023)

28. Rush uses the "MyRush powered by MyChart" website and mobile application to allow patients to access the MyChart patient portal, which is a software system designed and licensed to Rush by Epic Software Systems ("Epic").

29. Epic is a privately owned health care software company that provides services to 250 million patients, including two thirds of the US population.

30. Rush promises patients that Rush's MyChart patient portal is "private and secure."

> Is MyChart secure?
>
> We take great care to ensure your health information is kept private and secure. Access to information is controlled through secure activation codes, personal usernames and passwords. You control your own password, and your account cannot be accessed without that password. Further, MyChart uses the latest 128-bit SSL encryption technology with no caching to automatically encrypt your session

> with MyChart. Unlike conventional email, all MyChart messaging is done while you are securely logged on.[2]

31. Despite these promises, Rush knew that Epic's MyChart software system was designed to permit licensees—such as Rush—to deploy "custom analytics scripts" within MyChart including, for example, Google Analytics, which allows for the transmission of patients' personally identifiable information, including medical and health-related information, and communications to third parties.[3]

32. Rush took advantage of MyChart's analytics compatibility by knowingly and secretly deploying Google source code throughout its web properties, including inside the MyChart patient portal, that causes the contemporaneous unauthorized transmission of personally identifiable patient data and re-direction of the precise content of patient communications with Rush to be sent to Google whenever a Rush patient uses the Rush web properties, including the MyChart patient portal.

33. Like its other web properties, Rush actively encourages patients to use the MyChart patient portal.

34. As Rush patients and MyChart patient portal users, Plaintiffs exchanged communications with Rush through its web properties, including through the MyChart patient portal, each time Plaintiffs used the MyChart patient portal or other Rush web properties. Rush caused the contemporaneous unauthorized transmission of Plaintiffs' personally identifiable patient data and re-direction of the precise content of Plaintiffs' patient communications with Rush

[2] MyRush powered by MyChart, MyChart Frequently Asked Questions, available at https://mychart.rush.edu/MyChart/Authentication/Login?mode=stdfile&option=faq#AB_4 (last visited March 21, 2023).

[3] Feathers, T., *Pixel Hunt: Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022) (available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites).

to be sent to Google whenever Plaintiffs used the Rush web properties, including the MyChart patient portal.

IV. THE FORMS OF PATIENT PERSONALLY IDENTIFIABLE INFORMATION THAT RUSH CAUSES TO BE TRANSMITTED TO THIRD-PARTY MARKETING COMPANIES

35. Despite its own legal obligations and internal policies, Rush's source code causes the interception and transmission of the following personally identifiable information ("PII") to third parties whenever a patient uses Rush's web properties, including www.rush.edu and the MyChart patient portal:

a. Patient IP addresses;

b. Unique, persistent patient cookie identifiers;

c. Device identifiers;

d. Account numbers;

e. URLs;

f. Other unique identifying numbers, characteristics, or codes; and

g. Browser-fingerprints.

36. Whenever a patient uses Rush's web properties, including www.rush.edu and the MyChart patient portal, Rush intercepts, causes transmission of, and uses personally identifiable patient data without patient knowledge, consent, authorization, or any further action by the patient.

37. Despite its legal obligations, Rush's source code causes the interception and transmission of the precise content of patients' communications with Rush to third parties.

38. Rush discloses Plaintiffs' and Class members' personally identifiable patient data, including their status as patients and the contents of their communications with Rush, to third parties including Facebook, Google, and Bidtellect.

39. Rush's unauthorized disclosures to third parties includes information that identifies Plaintiffs and Class members as Rush patients and aids the third-parties in receiving and recording patient communications pertaining to or about specific doctors, conditions, treatments, payments, and connections to the MyChart patient portal.

40. Rush's third-party disclosures occur because Rush intentionally deploys source code at www.rush.edu, mychart.rush.edu, and inside Rush's MyChart patient portal that commandeers patients' web-browsers and causes personally identifiable patient data, as well as the exact contents of communications exchanged between Rush and Rush patients, to be sent to third parties.

41. Rush's third-party disclosures occur contemporaneous to communications with Plaintiff and Class members.

42. By design, the third-parties receive and record the exact contents of these communications before the full response from Rush to Plaintiffs or a Class member has been rendered on the screen of the patient's device and while the communication between Rush and patients remains ongoing.

43. Rush is not required to make disclosures to Facebook, Google, or Bidtellect for Rush's websites, including the patient portal, or services to function.

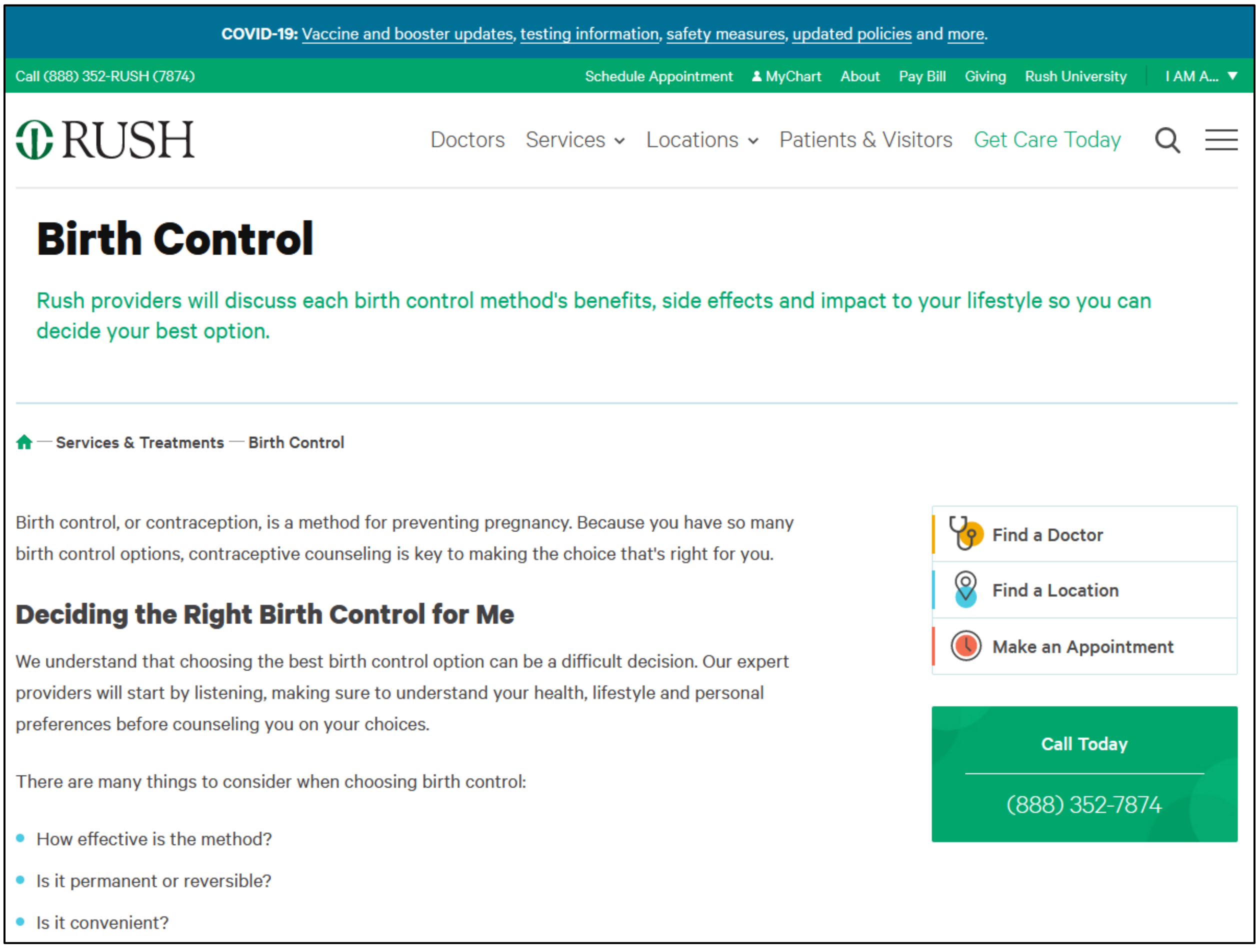
44. Rush causes transmission and disclosure of the precise content of patients' communications with Rush to third parties without patient knowledge, consent, authorization, or any further action by the patient.

V. RUSH SECRETLY TRANSMITS PERSONALLY IDENTIFIABLE PATIENT DATA AND RE-DIRECTS THE CONTENT OF PATIENT COMMUNICATIONS TO THIRD PARTIES

45. Web browsers are software applications that allow consumer to exchange electronic communications over the Internet.

46. Every website is hosted by a computer server through which the entity in charge of the website exchanges communications with Internet users via their web browsers.

47. The basic command web browsers use to communicate with website servers is called a GET request. As an example of how Rush uses GET requests to communicate, when a patient types in a Rush webpage such as https://www.rush.edu/treatments/birth-control into the navigation bar of her web-browser (or, just as, if not more frequently, takes the technological shortcut of clicking a preset hyperlink to the page), the patient's web-browser makes connection with the server for Rush and sends the following: "GET /treatments/birth-control HTTP/1.1" and the following webpage loads on the patient's browser:



COVID-19: Vaccine and booster updates, testing information, safety measures, updated policies and more.

Call (888) 352-RUSH (7874)

Birth Control

Rush providers will discuss each birth control method's benefits, side effects and impact to your lifestyle so you can decide your best option.

Birth control, or contraception, is a method for preventing pregnancy. Because you have so many birth control options, contraceptive counseling is key to making the choice that's right for you.

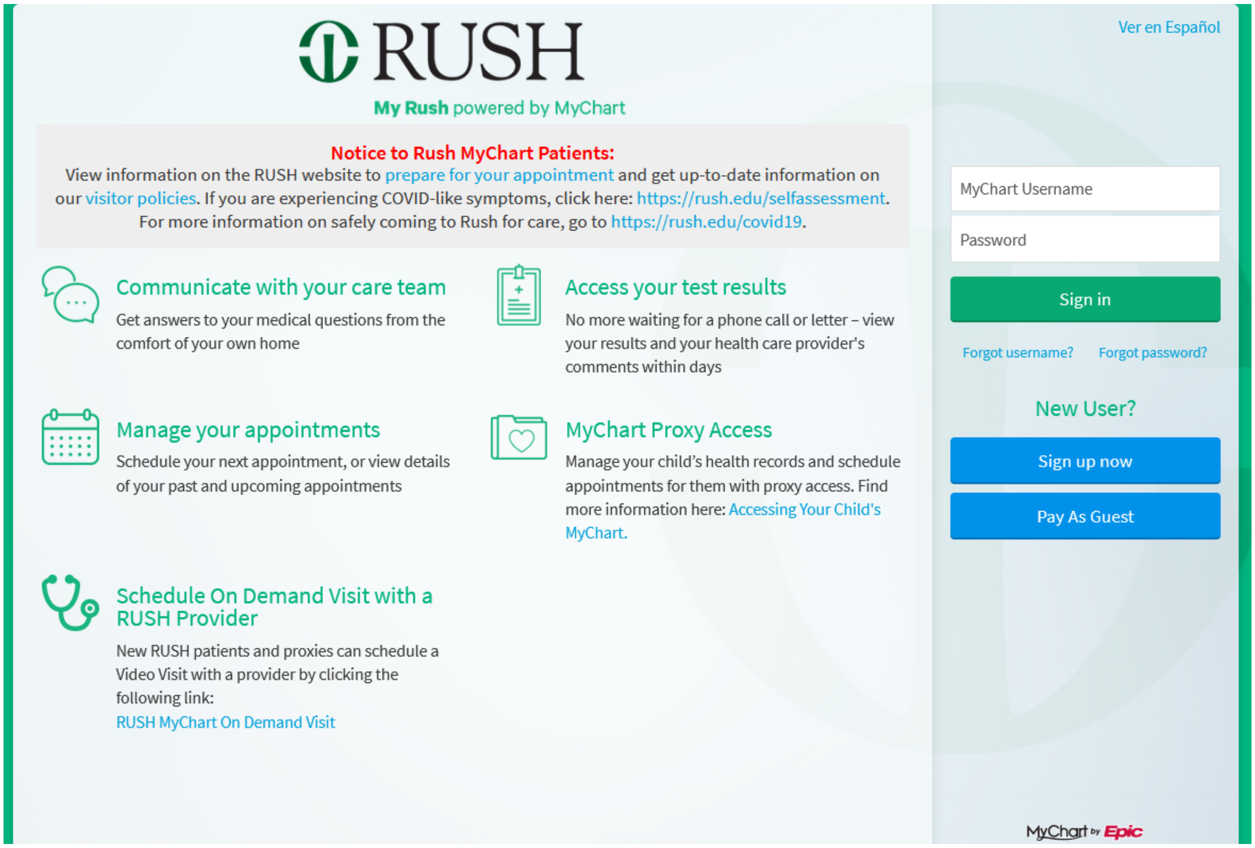
Deciding the Right Birth Control for Me

We understand that choosing the best birth control option can be a difficult decision. Our expert providers will start by listening, making sure to understand your health, lifestyle and personal preferences before counseling you on your choices.

There are many things to consider when choosing birth control:

- How effective is the method?
- Is it permanent or reversible?
- Is it convenient?

48. Upon accessing the login for the Rush MyChart Patient Portal, the GET command is used and the below sequence of pages is displayed. First, the login landing page, called with the request "GET /mychart/Authentication/Login?%5Fga=[_ga cookie hex value] HTTP/1.1".



RUSH

My Rush powered by MyChart

Notice to Rush MyChart Patients:

View information on the RUSH website to prepare for your appointment and get up-to-date information on our visitor policies. If you are experiencing COVID-like symptoms, click here: https://rush.edu/selfassessment. For more information on safely coming to Rush for care, go to https://rush.edu/covid19.

Communicate with your care team

Get answers to your medical questions from the comfort of your own home

Access your test results

No more waiting for a phone call or letter – view your results and your health care provider's comments within days

Manage your appointments

Schedule your next appointment, or view details of your past and upcoming appointments

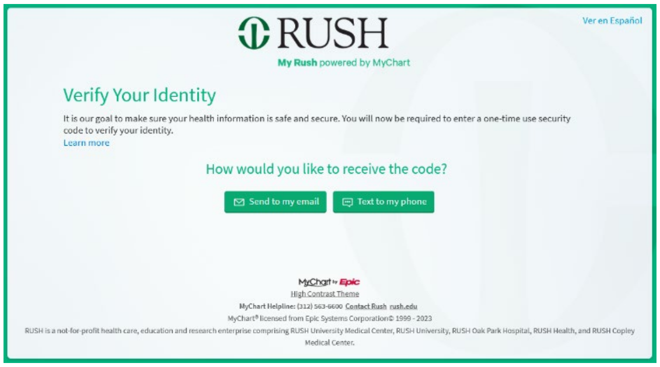
MyChart Proxy Access

Manage your child's health records and schedule appointments for them with proxy access. Find more information here: Accessing Your Child's MyChart.

Schedule On Demand Visit with a RUSH Provider

New RUSH patients and proxies can schedule a Video Visit with a provider by clicking the following link:
RUSH MyChart On Demand Visit

Next, the login process requires a second factor of authentication, usually a numeric code sent to the user via text or email. The below pages are called with the request command "GET /MyChart/Authentication/SecondaryValidation HTTP/1.1" and "GET /MyChart/areas/authentication/templates/twofactordescription.tmpl.js?updateDt=[epoch time and date stamp] HTTP/1.1" respectively.

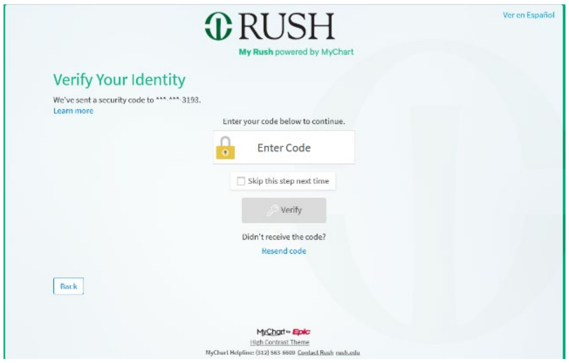


Verify Your Identity

It is our goal to make sure your health information is safe and secure. You will now be required to enter a one-time use security code to verify your identity.
Learn more

How would you like to receive the code?

MyChart Helpline: (312) 563-6600 Contact Rush rush.edu
MyChart® licensed from Epic Systems Corporation© 1999 - 2023
RUSH is a not-for-profit health care, education and research enterprise comprising RUSH University Medical Center, RUSH University, RUSH Oak Park Hospital, RUSH Health, and RUSH Copley Medical Center.



Verify Your Identity

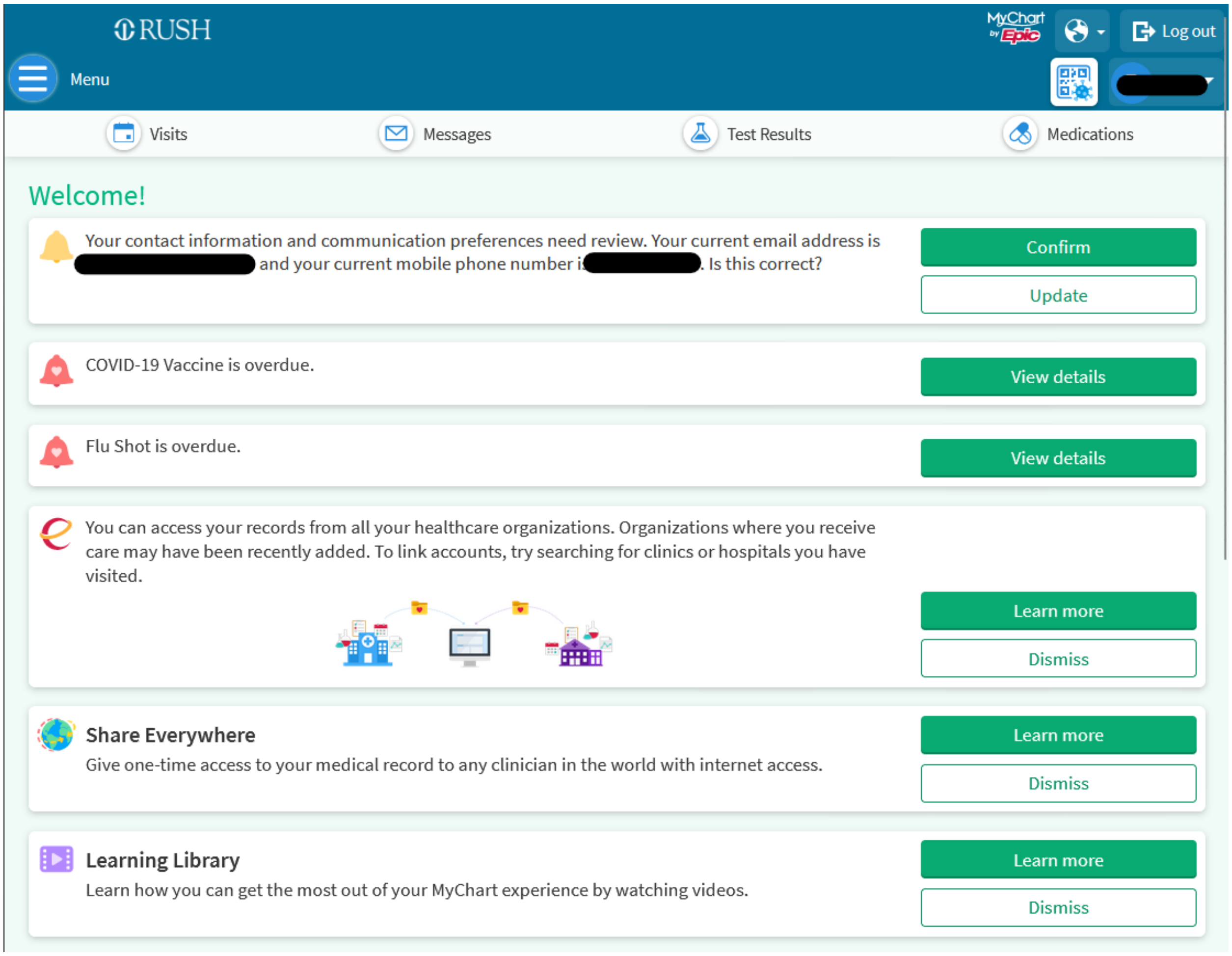
We've sent a security code to ***-***-3193.
Learn more

Enter your code below to continue.

Didn't receive the code?
Resend code

MyChart Helpline: (312) 563-6600 Contact Rush rush.edu

Finally, upon providing the second factor authentication code, the user lands on the home page of the Rush Patient Portal, as displayed below. This page uses the request "GET /MyChart/Home/ HTTP/1.1".



Welcome!

Your contact information and communication preferences need review. Your current email address is [redacted] and your current mobile phone number i[redacted]. Is this correct?

COVID-19 Vaccine is overdue.

Flu Shot is overdue.

You can access your records from all your healthcare organizations. Organizations where you receive care may have been recently added. To link accounts, try searching for clinics or hospitals you have visited.

Share Everywhere
Give one-time access to your medical record to any clinician in the world with internet access.

Learning Library
Learn how you can get the most out of your MyChart experience by watching videos.

49. The other basic request utilized by web browsers is a POST request, which is typically employed when a user enters data into a form on a website and clicks 'Enter' or a submit button. 'POST' sends the data entered in the form to the server for the website.

50. In response to receiving a GET or POST request, the server for the entity with which the user is exchanging communications, in this case Rush's server, will send a set of instructions to the web-browser, commanding the browser with source code that (1) directs the browser on how to render the entity's response and, in many circumstances, (2) commands the browser to transmit personally identifiable data about the Internet user and re-direct the precise content of the user's GET or POST requests to various third parties.

51. In addition to these communications between Rush and the patient, however, when a patient communicates with Rush's website (whether by typing in a webpage, putting in a search, clicking on a hyperlink, logging into the MyChart patient portal, maneuvering through the patient portal, or otherwise), Rush also causes some of that information to be transmitted to third parties without the patient's knowledge or authorization. The third parties to whom user data is transmitted and the content of communications redirected are typically procured by websites to track users' personally identifiable data and communications for marketing purposes, i.e. targeted advertising.

52. In many such cases, the third parties acquire the content of user communications through a 1x1 pixel (the smallest dot on a user's screen) called a web bug, tracking pixel, or web beacon. These web-bugs are tiny and purposefully camouflaged to remain invisible to the user.

53. Web bugs can be placed directly on a page by a web developer or can be funneled through a "tag manager" service to make the invisible tracking run more efficiently and to further

obscure the third parties to whom the website transmits personally identifiable user data and re-directs the content of communications.

54. In the absence of a tag manager, a website developer who chooses to deploy third party source code on their website must enter the third-party source code directly onto their website for every third-party to whom they seek to transmit and re-direct user data and communications. On websites with several third-party trackers, this may cause the page to load more slowly and increases risk of a coding error, effecting functionality and usability. A "tag manager" offers the website developer a container in which to place all third-party source code. Instead of placing all third-party source code directly on the webpage, the developer places the source code within its account at the tag manager.

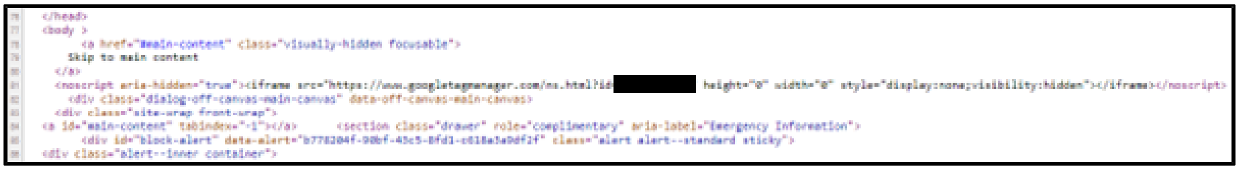
55. Google explains the benefits of Google Tag Manager in an Introduction to Google Tag Manager video on YouTube. [4] Google explains:

> Tags on your website help you measure traffic and optimize your online marketing. But all that code is cumbersome to manage. It often takes too long to get new tags on your site or update existing ones. This can delay campaigns by weeks or months so you miss valuable opportunities, data, and sales. That's where tag management comes in. Google Tag Manager is a powerful free tool that puts you the marketer back in control of your digital marketing. You update all your tags from Google Tag Manager instead of editing the site code. This reduces errors, frees you from having to involve a web master, and lets you quickly deploy tags on your site.
>
> Here's how it works. Sign in with an existing Google Account. Go to Google.com/tagmanager and create an account for your company. We'll name this one after the name of our company, Example Inc. Next, create a container for your domain name. We'll name this one after our website, example.com. This container will hold all the tags on the site. When you create a container, Google Tag Manager generates a container snippet to add to your site. Copy this container snippet and paste it into every page of your site. Paste the snippet below the opening body tag. Once you've pasted the container snippet into your site, you add and edit your tags using Google Tag Manager. You can add any marketing or measurement tag you want, whenever you want.

[4] See https://www.youtube.com/watch?v=KRvbFpeZ11Y, audio from 0:04 to 1:40.

56. Rush deploys Google Tag Manager on its websites through an "iframe," a nested "frame" that exists within the Rush web properties, including inside Rush's MyChart patient portal, that is, in reality, an invisible window through which Rush funnels web bugs for third parties to secretly acquire the content of patient communications without any knowledge, consent, authorization, or further action of patients.

57. Rush's Google Tag Manager source code is designed to be invisible. For example, on the "birth control" communications page set forth above, the GTM source code used by Rush specifies an "iframe" with a height of 0, width of 0, display of none, and visibility of hidden.



```
</head>
<body >
        <a href="#main-content" class="visually-hidden focusable">
      Skip to main content
    </a>
    <noscript aria-hidden="true"><iframe src="https://www.googletagmanager.com/ns.html?id=[redacted] height="0" width="0" style="display:none;visibility:hidden"></iframe></noscript>
      <div class="dialog-off-canvas-main-canvas" data-off-canvas-main-canvas>
    <div class="site-wrap front-wrap">
<a id="main-content" tabindex="-1"></a>        <section class="drawer" role="complimentary" aria-label="Emergency Information">
        <div id="block-alert" data-alert="b778204f-90bf-45c5-8fd1-c618a5a9df2f" class="alert alert--standard sticky">
<div class="alert--inner container">
```

58. Rush then funnels invisible 1x1 web bugs or pixels through this purposefully invisible iframe to help third-parties track, acquire, and record patient data and communications.

59. By design, none of the tracking is visible to patients at the Rush web properties.

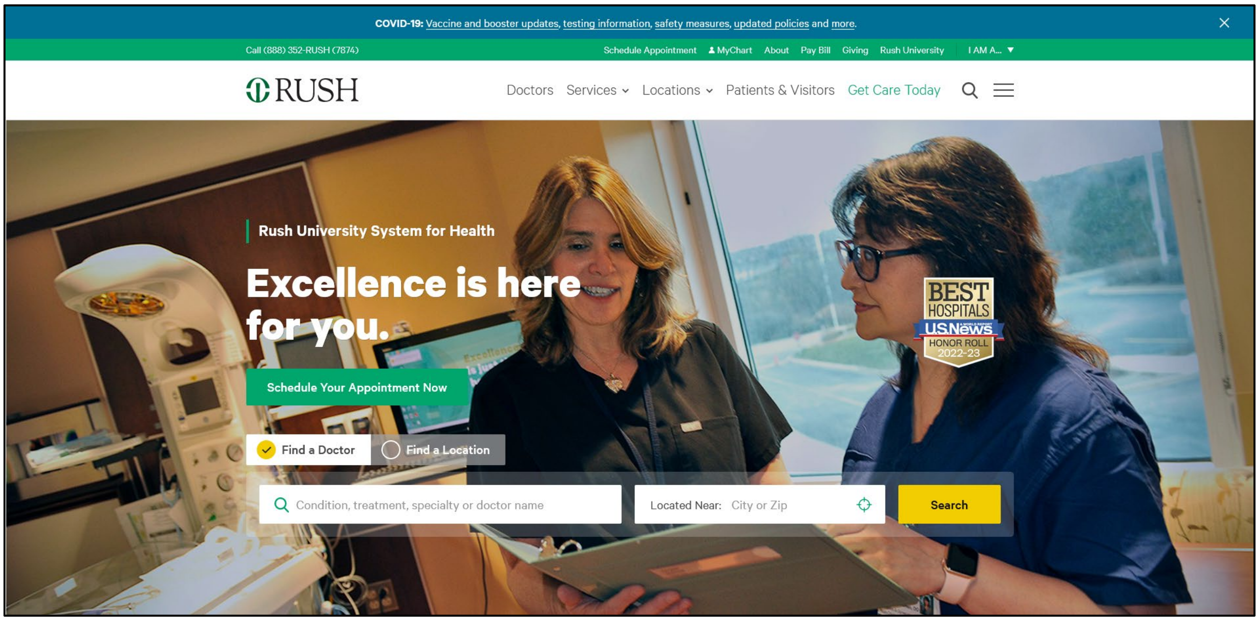
60. For example, the reproductive medicine page above does not include anything to apprise patients that Rush is causing their personally identifiable data to be transmitted and the content of their communications re-directed to third parties including Facebook and Google.

VI. WHAT HAPPENS WHEN A PATIENT COMMUNICATES WITH RUSH AT RUSH'S WEB PROPERTIES

61. "Fiddler" is a commercially available software application used by web developers to test how their various applications and source codes operate. By using Fiddler, one can also capture and record communications and other data transmissions that flow to and from a web-browser over the Internet. The following is derived from a test Fiddler analysis in connection with the www.rush.edu web property.

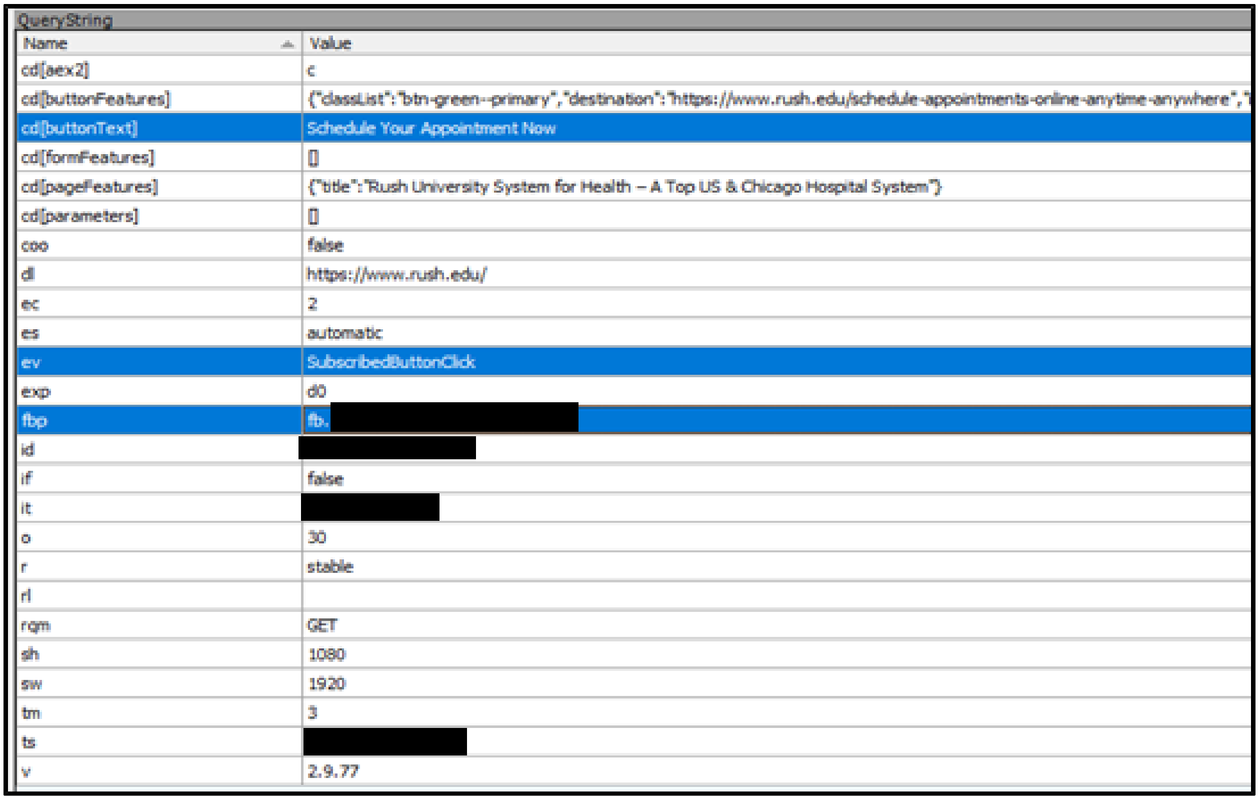
62. When a patient first visits the www.rush.edu homepage, the source code that Rush utilizes causes personally identifiable patient data to be transmitted and the contents of patient communications to be re-direct to third parties connected to the fact that the patient is present at the Rush property.

63. Many of the tabs provided by Rush on its web properties are specific to patients—i.e. "Schedule Your Appointment Now," "Pay Your Bill," "Medical Records," "Connect With Rush," and "Plan Your Stay," among others (collectively "Patient Tabs"). Clicking on any of the Patient Tabs identifies the person using the web property as a patient for purposes of using the Rush web property:


COVID-19: Vaccine and booster updates, testing information, safety measures, updated policies and more.

64. When a patient clicks the tab to "Schedule Your Appointment Now," Rush causes the transmission of the patient's personally identifiable data and re-directs the content of the patient's click of the "Schedule Your Appointment Now" button to Facebook.

65. For example, Fiddler shows the following types of data are transmitted to Facebook through a test "formPOST" request caused by Rush's source code whenever a patient clicks on the Schedule Your Appointment Now link:



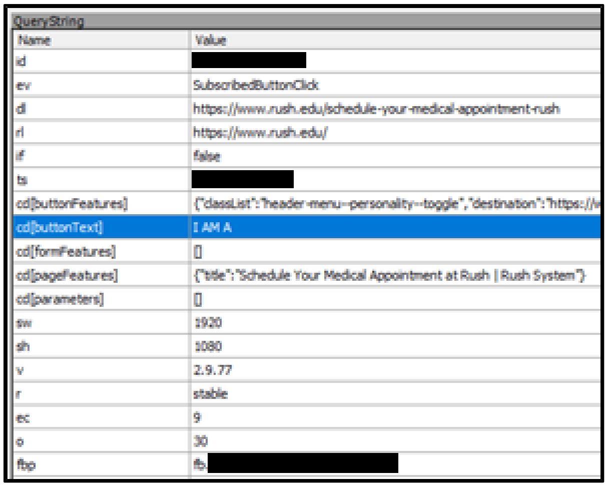
QueryString

Name	Value
cd[aex2]	c
cd[buttonFeatures]	{"classList":"btn-green--primary","destination":"https://www.rush.edu/schedule-appointments-online-anytime-anywhere","
cd[buttonText]	Schedule Your Appointment Now
cd[formFeatures]	[]
cd[pageFeatures]	{"title":"Rush University System for Health – A Top US & Chicago Hospital System"}
cd[parameters]	[]
coo	false
dl	https://www.rush.edu/
ec	2
es	automatic
ev	SubscribedButtonClick
exp	d0
fbp	fb.[redacted]
id	[redacted]
if	false
it	[redacted]
o	30
r	stable
rl	
rqm	GET
sh	1080
sw	1920
tm	3
ts	[redacted]
v	2.9.77

This chart shows disclosure to Facebook that the patient engaged in an event ('ev') labeled "SubscribedButtonClick," that the "buttonText" was "Schedule Your Appointment Now," that the button was clicked from https://www.rush.edu, and the details of the first-party _fbp cookie assigned by Rush.

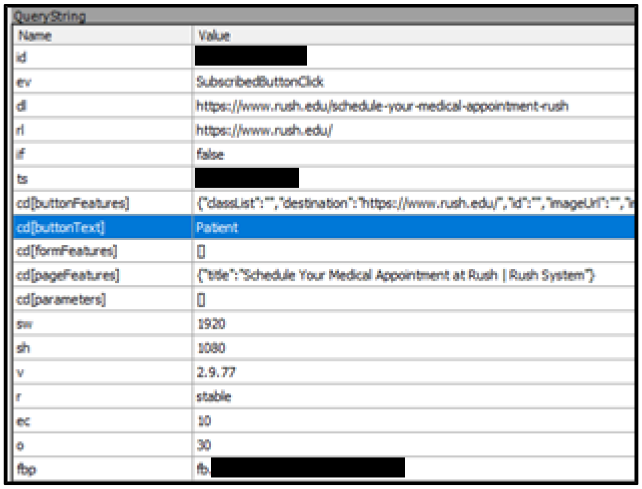
66. Rush causes multiple data transmissions containing personally identifiable patient information to be made to Facebook before the data is sent to Rush.

67. Rush does not just disclose patient status to Facebook implicitly through the transmission of MyChart-related activity, but directly by transmitting the text "I AM A … Patient" to Facebook in successive transmissions:



QueryString

Name	Value
id	[redacted]
ev	SubscribedButtonClick
dl	https://www.rush.edu/schedule-your-medical-appointment-rush
rl	https://www.rush.edu/
if	false
ts	[redacted]
cd[buttonFeatures]	{"classList":"header-menu--personality--toggle","destination":"https://w
cd[buttonText]	I AM A
cd[formFeatures]	[]
cd[pageFeatures]	{"title":"Schedule Your Medical Appointment at Rush | Rush System"}
cd[parameters]	[]
sw	1920
sh	1080
v	2.9.77
r	stable
ec	9
o	30
fbp	fb.[redacted]



QueryString

Name	Value
id	[redacted]
ev	SubscribedButtonClick
dl	https://www.rush.edu/schedule-your-medical-appointment-rush
rl	https://www.rush.edu/
if	false
ts	[redacted]
cd[buttonFeatures]	{"classList":"","destination":"https://www.rush.edu/","id":"","imageUrl":"","i
cd[buttonText]	Patient
cd[formFeatures]	[]
cd[pageFeatures]	{"title":"Schedule Your Medical Appointment at Rush | Rush System"}
cd[parameters]	[]
sw	1920
sh	1080
v	2.9.77
r	stable
ec	10
o	30
fbp	fb.[redacted]

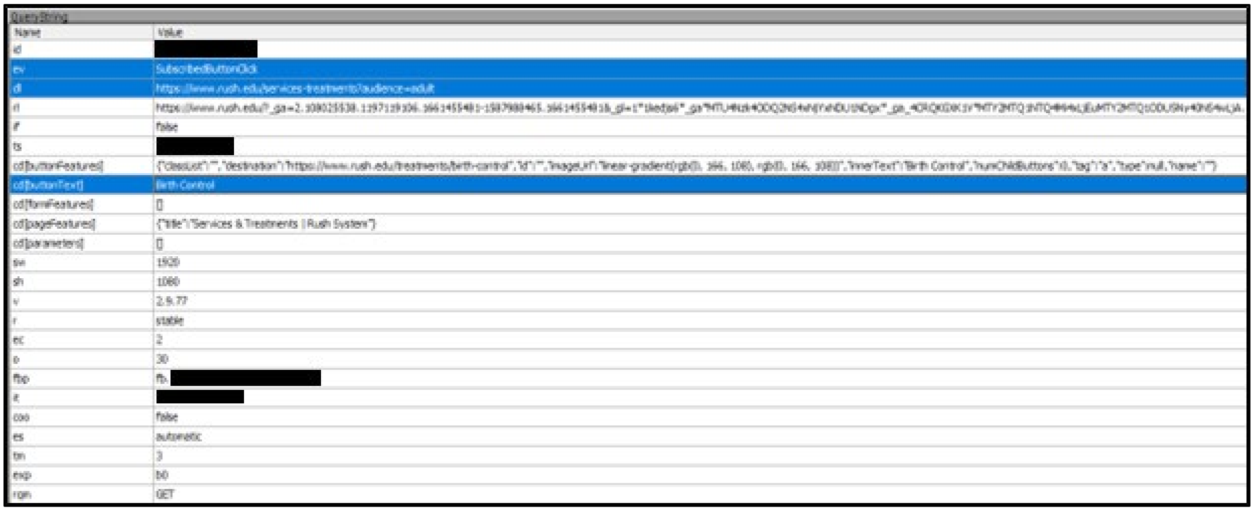
68. Rush causes similar data transmissions to be sent to Facebook with every communication that a patient sends using the Patient Tabs.

69. Rush also causes similar data transmissions to be sent to Facebook with every communication that a patient sends at its www.rush.edu web property generally.

70. For example, when a patient sends a communication searching for more information on "birth control" (or any other search), Rush causes data transmissions to be made to third parties, including Facebook, Google, and Bidtellect, that include personally identifiable patient data and the content of the patient's re-directed communication.

71. Immediately upon a patient sending the "birth control" communication to Rush, the source code triggers separate contemporaneous data transmissions containing personally identifiable patient data and the content of the patient's communication to third parties, including Facebook, Google, and Bidtellect.

72. An example transmission to Facebook includes the following:

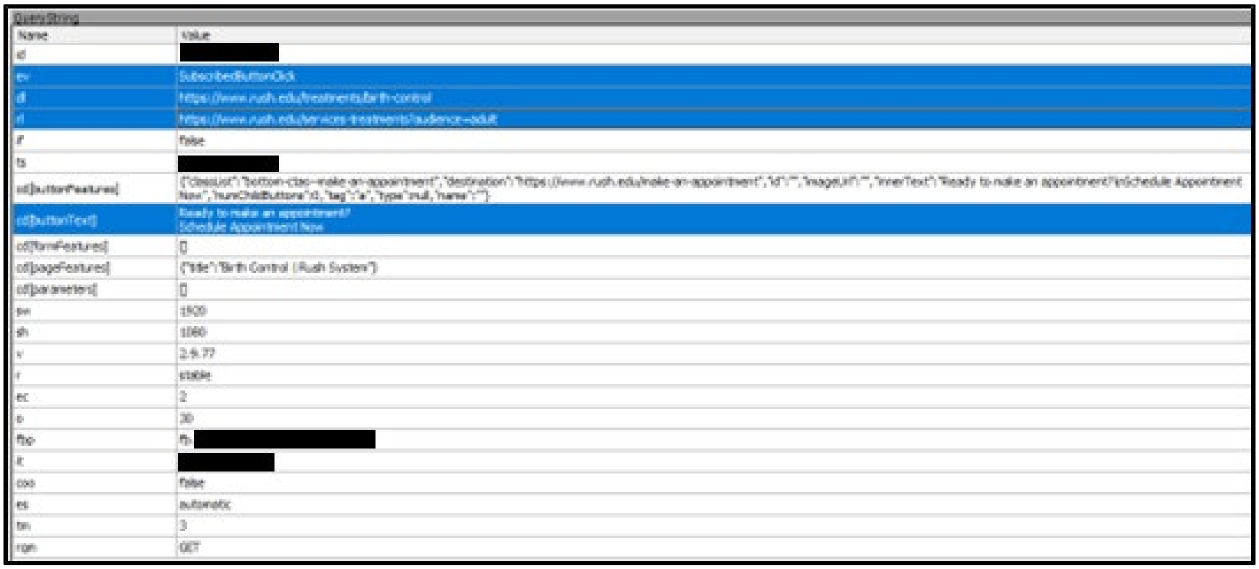


QueryString

Name	Value
id	[redacted]
ev	SubscribedButtonClick
dl	https://www.rush.edu/services-treatments?audience=adult
rl	https://www.rush.edu/?_ga=2.108025538.1197119106.1661455481-1587988465.1661455481&_gl=1*1ked6i6*_ga*MTU4NzkwODQ2NS4xNjYxNDU1NDgx*_ga_4ORQXDK1V*MTY2MTQ1NTQ4MS4xLjEuMTY2MTQ1ODU5Ny40NS4wLjA.
if	false
ts	[redacted]
cd[buttonFeatures]	{"classList":"","destination":"https://www.rush.edu/treatments/birth-control","id":"","imageUrl":"linear-gradient(rgb(0, 166, 108), rgb(0, 166, 108))","innerText":"Birth Control","numChildButtons":0,"tag":"a","type":null,"name":""}
cd[buttonText]	Birth Control
cd[formFeatures]	[]
cd[pageFeatures]	{"title":"Services & Treatments | Rush System"}
cd[parameters]	[]
sw	1920
sh	1080
v	2.9.77
r	stable
ec	2
o	30
fbp	fb.[redacted]
it	[redacted]
coo	false
es	automatic
tm	3
exp	b0
rqm	GET

This shows that the patient has engaged in a "SubscribedButtonClick," that the text of the button was "Birth Control," that the patient sending the request was an adult (*i.e.* audience=adult), the patient's unique Google Analytics identifier, and the patient's unique Facebook Pixel identifier.

73. If the patient continues his or her browsing session to schedule an appointment, Rush transmits the appointment request to Facebook:

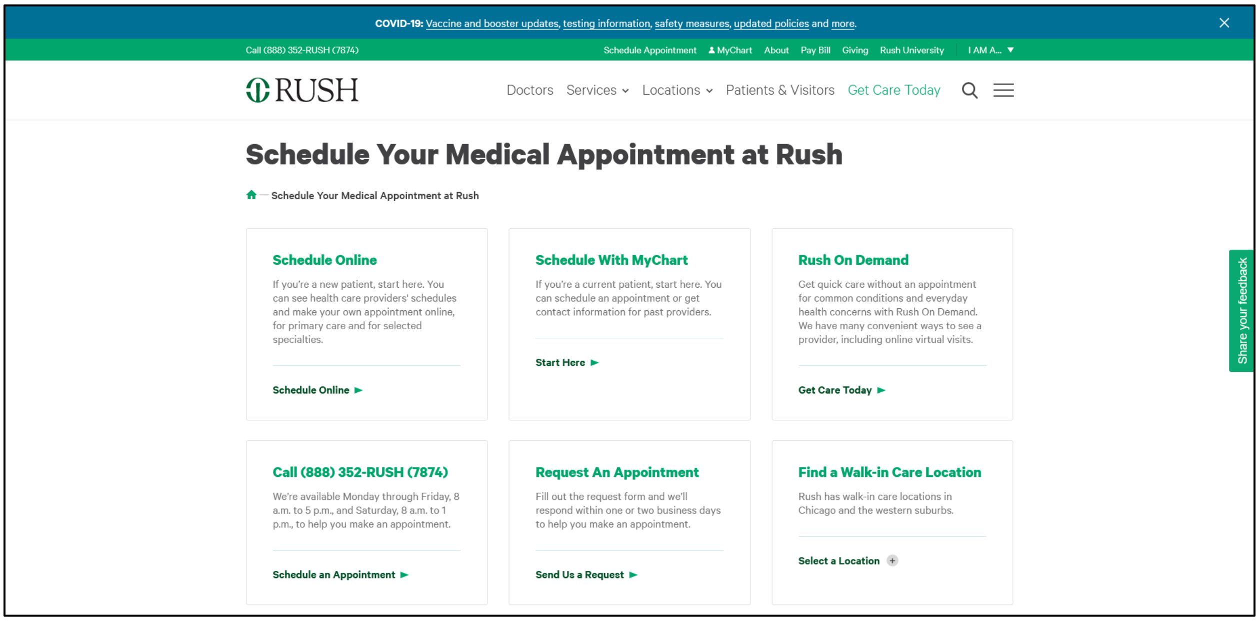


QueryString

Name	Value
id	[redacted]
ev	SubscribedButtonClick
dl	https://www.rush.edu/treatments/birth-control
rl	https://www.rush.edu/services-treatments?audience=adult
if	false
ts	[redacted]
cd[buttonFeatures]	{"classList":"button-cta--make-an-appointment","destination":"https://www.rush.edu/make-an-appointment","id":"","imageUrl":"","innerText":"Ready to make an appointment?\nSchedule Appointment Now","numChildButtons":0,"tag":"a","type":null,"name":""}
cd[buttonText]	Ready to make an appointment? Schedule Appointment Now
cd[formFeatures]	[]
cd[pageFeatures]	{"title":"Birth Control | Rush System"}
cd[parameters]	[]
sw	1920
sh	1080
v	2.9.77
r	stable
ec	2
o	30
fbp	fb.[redacted]
it	[redacted]
coo	false
es	automatic
tm	3
rqm	GET

This shows Rush has caused disclosure that the patient has engaged in a "SubscribedButtonClick," that the text of the button was "Ready to make an appointment? Schedule Appointment Now," that the user was visiting the "birth control" page of the Rush web property and the patient's Facebook Pixel identifier.

74. However, all of these transmissions are hidden from the patient. Instead, the patient only sees the following page rendered, without an indication of third-party disclosures:



COVID-19: Vaccine and booster updates, testing information, safety measures, updated policies and more.

Call (888) 352-RUSH (7874)

Schedule Your Medical Appointment at Rush

— Schedule Your Medical Appointment at Rush

Schedule Online

If you're a new patient, start here. You can see health care providers' schedules and make your own appointment online, for primary care and for selected specialties.

Schedule Online ►

Schedule With MyChart

If you're a current patient, start here. You can schedule an appointment or get contact information for past providers.

Start Here ►

Rush On Demand

Get quick care without an appointment for common conditions and everyday health concerns with Rush On Demand. We have many convenient ways to see a provider, including online virtual visits.

Get Care Today ►

Call (888) 352-RUSH (7874)

We're available Monday through Friday, 8 a.m. to 5 p.m., and Saturday, 8 a.m. to 1 p.m., to help you make an appointment.

Schedule an Appointment ►

Request An Appointment

Fill out the request form and we'll respond within one or two business days to help you make an appointment.

Send Us a Request ►

Find a Walk-in Care Location

Rush has walk-in care locations in Chicago and the western suburbs.

Select a Location +

75. Regardless of the next link a patient clicks to continue its communication with Rush at the Rush web-property, the source code purposefully deployed by Rush will cause transmission of their personally identifiable patient data and simultaneously re-direct the specific contents of their communication to third parties including Facebook, Google, and Bidtellect.

76. Rush uses the same tools and source code throughout its web properties, and the types of personally identifiable patient data and contents of patient communications contents Fiddler analysis determined were being transmitted to third parties without patient knowledge or authorization from the main www.rush.edu page, the Schedule Your Appointment Now link, and the birth control information page, are transmitted every time a Rush patient uses the Rush web properties, regardless of where the patient goes on the Rush websites.

How It Works

77. To make the transmissions of patient information and communications to Facebook and Google, Rush deploys or deployed Facebook and Google source code on its web properties.

78. The Rush-deployed source code does the following things:

a. Without any action or authorization, Rush deposits cookies named _fbp, _ga, and _gid onto Plaintiffs and patient Class members' computing devices. These are cookies associated with the third-parties Facebook and Google but which Rush deposits on Plaintiffs and Class members' computing devices by disguising them as first-party cookies.

b. Without any action or authorization, Rush commands Plaintiffs' and Class members' computing devices to contemporaneously re-direct the Plaintiffs' and Class members' identifiers and the content of their communications to Facebook, Google, and others.

VII. THE THIRD PARTIES TO WHOM RUSH CAUSES DISCLOSURES OF PATIENT COMMUNICATIONS AND PII INCLUDE GOOGLE AND FACEBOOK

A. <u>Google</u>

79. By many measures, Google is the world's largest data company. Among other services, Google operates the world's most popular search engine (Google), email provider (Gmail), video website (YouTube), mapping service (Google Maps), Internet analytics service for web developers (Google Analytics), and web-browser (Chrome). It also operates various ad services that are among the world's most popular in their respective category, including the advertising services of Google DoubleClick and Google AdWords.

80. Google Analytics has massive reach. As described by the Wall Street Journal, it is "far and away the web's most dominant analytics platform" and "tracks you whether or not you are logged in."[5]

81. Google tracks Internet users with IP addresses, cookies, geolocation, and other unique device identifiers.

82. Google cookies are personally identifiable. For example, Google explains the following about certain cookies that it uses:

a. "[C]ookies called 'SID' and 'HSID' contain digitally signed and encrypted records of a user's Google account ID and most recent sign-in time."[6]

b. "Most people who use Google services have a preferences cookie called 'NID' in their browsers. When you visit a Google service, the browser sends this cookie with your request for a page. The NID cookie contains a unique ID Google uses to remember your preferences and other information[.]"[7]

c. "We use cookies like NID and SID to help customize ads on Google properties, like Google Search. For example, we use such cookies to remember your most recent searches, your previous interactions with an advertiser's ads or search results, and your visits to an advertiser's website. This helps us to show you customized ads on Google."[8]

[5] *Who Has More of Your Personal Data than Facebook? Try Google*, The Wall Street Journal (April 22, 2018) (available at https://www.wsj.com/articles/who-has-more-of-your-personal-data-than-facebook-try-google-1524398401).

[6] *Privacy & Terms, Types of Cookies Used by Google*, Google, http://web.archive.org/web/20210916060858/https:/policies.google.com/technologies/cookies?hl=en-US (archived from September 16, 2021).

[7] *Privacy & Terms, Types of Cookies Used by Google*, Google, http://web.archive.org/web/20210101020222/https:/policies.google.com/technologies/cookies?hl=en-US (archived from January 1, 2021).

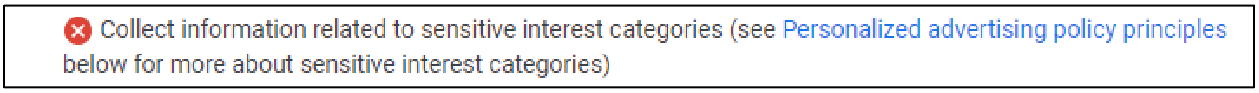
[8] *Id.*

d. “We also use one or more cookies for advertising we serve across the web. One of the main advertising cookies on non-Google sites is named ‘IDE’ and is stored in browsers under the domain doubleclick.net. Another is stored in google.com and is called ANID. We use other cookies with names such as DSID, FLC, AID, TAID, and exchange_uid. Other Google properties, like YouTube, may also use these cookies to show you more relevant ads.”[9]

83. Google warns web-developers that Google marketing tools are not appropriate for every type of website or webpage, including health-related webpages and websites.

84. Google warns developers in its Personalized Advertising policies page that “Health in personalized advertising” is a “Prohibited category” for Google’s personalized advertising tools. Specifically, Google’s advertising policies page states:[10]

> We take user privacy very seriously, and we also expect advertisers to respect user privacy. These policies define how advertisers are allowed to collect user data and use it for personalized advertising. They apply to advertisers using targeting features, including remarketing, affinity audiences, custom affinity audiences, in-market audiences, similar audiences, demographic and location targeting, and keyword contextual targeting. …
>
> You aren’t allowed to do the following:

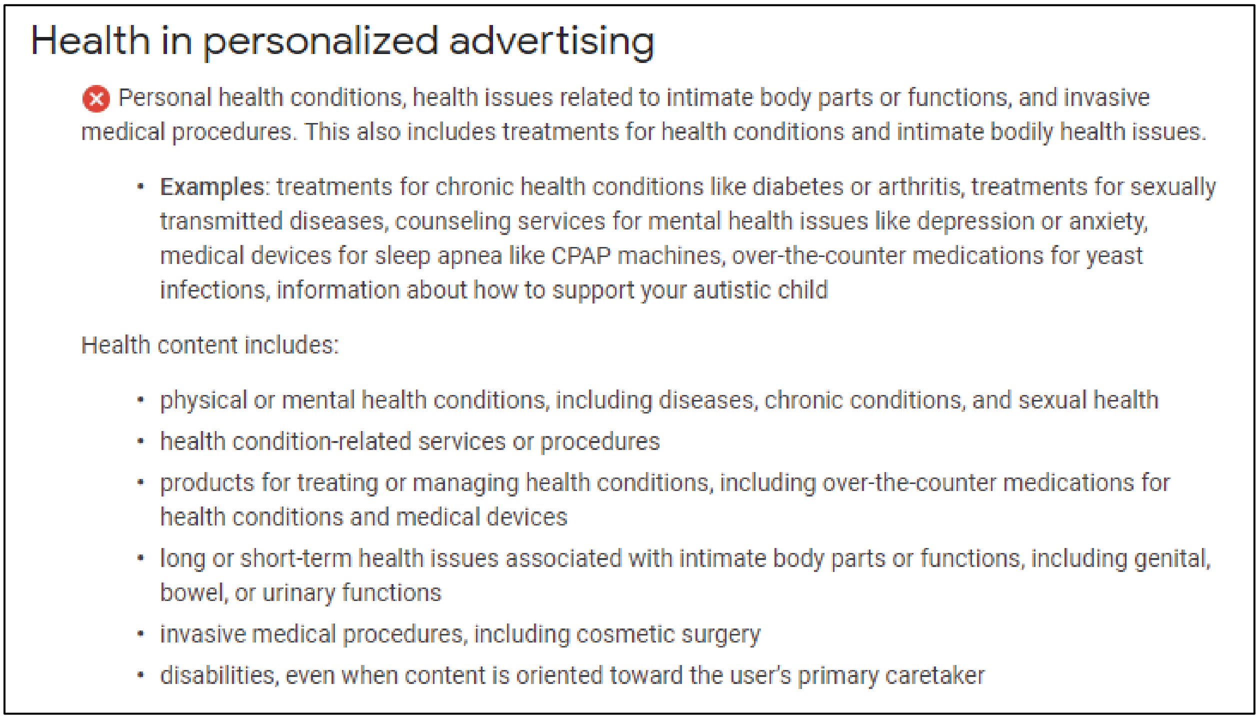


⊗ Collect information related to sensitive interest categories (see Personalized advertising policy principles below for more about sensitive interest categories)

85. Google further states that “[a]dvertisers can’t use sensitive interest categories to target ads or to promote advertisers’ products or services.”[11] “Health” is one such “[p]rohibited

[9] *Id.*
[10] *Advertising Policies Help, Personalized Advertising*, Google, http://web.archive.org/web/20191031223446/https://support.google.com/adspolicy/answer/143465?hl=en (archived from October 31, 2019).
[11] *Id.*

categor[y]" that Google states "can't be used by advertisers to targets ads to users or promote advertisers' products or services."



Health in personalized advertising

⊗ Personal health conditions, health issues related to intimate body parts or functions, and invasive medical procedures. This also includes treatments for health conditions and intimate bodily health issues.

- **Examples**: treatments for chronic health conditions like diabetes or arthritis, treatments for sexually transmitted diseases, counseling services for mental health issues like depression or anxiety, medical devices for sleep apnea like CPAP machines, over-the-counter medications for yeast infections, information about how to support your autistic child

Health content includes:

- physical or mental health conditions, including diseases, chronic conditions, and sexual health
- health condition-related services or procedures
- products for treating or managing health conditions, including over-the-counter medications for health conditions and medical devices
- long or short-term health issues associated with intimate body parts or functions, including genital, bowel, or urinary functions
- invasive medical procedures, including cosmetic surgery
- disabilities, even when content is oriented toward the user's primary caretaker

86. Google provides instructions for web developers to anonymize IP addresses when they use Google Analytics.[12] Google explains that the IP anonymization feature "is designed to help site owners comply with their own privacy policies or, in some countries, recommendations from local data protection authorities, which may prevent the storage of full IP address information."[13] The Google IP anonymization instructions tell web developers to add a parameter called 'aip' in their Google Analytics source code. When 'aip' ("anonymize IP") is turned on, it will be reported to Google Analytics in a GET request with the following: '&aip=1'.[14]

[12] *Analytics Help, IP Anonymization (or IP Masking) in Universal Analytics*, Google, https://support.google.com/analytics/answer/2763052?hl=en

[13] *Id.*

[14] *Id.*

87. Upon information and belief, Rush does not use Google's IP anonymization tool with Google Analytics. As a result, Rush's use of Google Analytics is not anonymous, even when no cookies are involved in the re-direction of a patient's communication.

88. Rush deploys Google tracking tools on nearly every page on its web properties, including within the MyChart patient portal, thereby causing disclosure of communications exchanged with patients to be re-directed to Google.

89. Each time a Rush patient, including Plaintiffs and Class members, visited the Rush web properties, including www.rush.edu, www.mychart.rush.edu, and inside the MyChart patient portal, Rush caused the disclosure of communications exchanged with the patient to be re-directed to Google.

B. Facebook

90. Facebook operates the world's largest social media company.

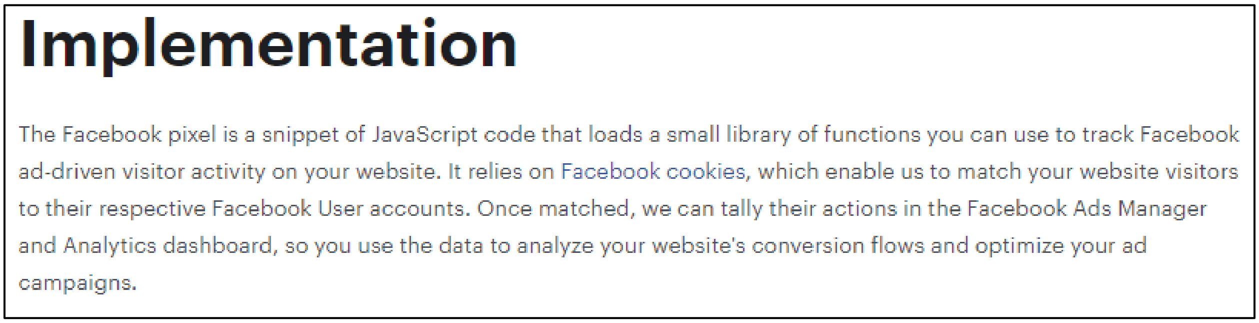
91. Facebook maintains profiles on users that include users' real names, locations, email addresses, friends, likes, and communications that Facebook associates with personal identifiers including IP addresses and cookie identifiers.

92. Facebook also tracks non-users across the web through its widespread Internet marketing products and source code.

93. Facebook's revenue is derived almost entirely from selling targeted advertising to Facebook users on Facebook.com and to all Internet users on non-Facebook sites that integrate Facebook marketing source code on their websites.

94. The Facebook Tracking Pixel (a/k/a the "Meta Pixel") is an invisible 1x1 web bug that Facebook makes available to web-developers to help developers track Facebook and other ad-driven activity on their website. Facebook warns developers that the Facebook Pixel is a personal

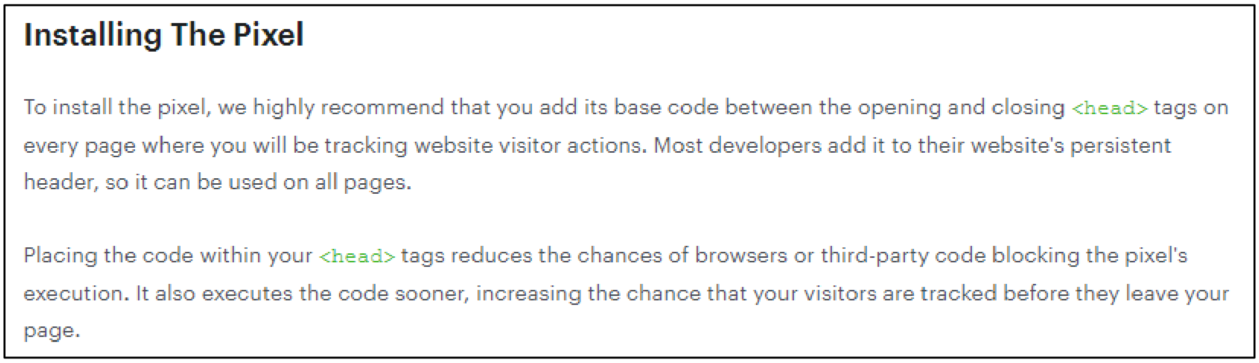
identifier because it "relies on Facebook cookies, which enable [Facebook] to match your website visitors to their respective Facebook User accounts."



Implementation

The Facebook pixel is a snippet of JavaScript code that loads a small library of functions you can use to track Facebook ad-driven visitor activity on your website. It relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can tally their actions in the Facebook Ads Manager and Analytics dashboard, so you use the data to analyze your website's conversion flows and optimize your ad campaigns.

95. Facebook recommends that the pixel code be placed early in the source code for any given webpage or website to ensure that the user will be tracked:



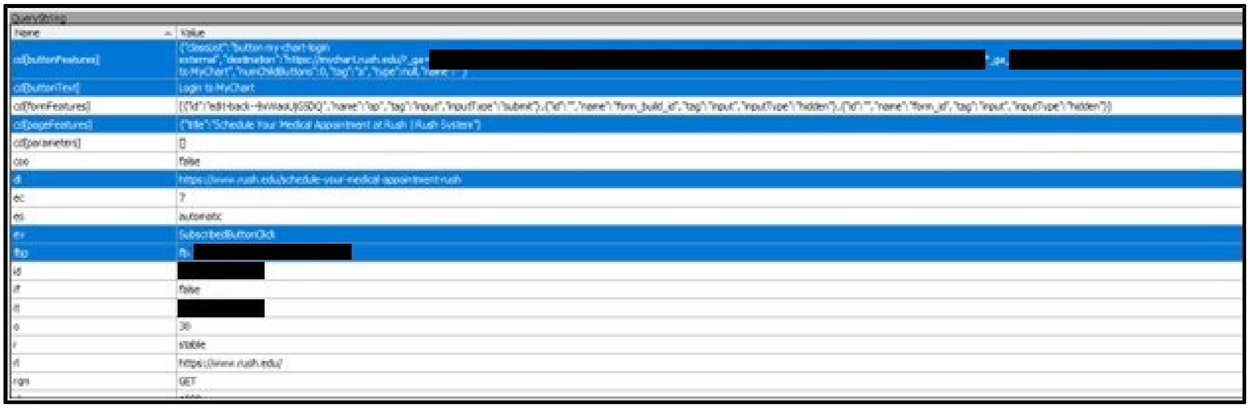
Installing The Pixel

To install the pixel, we highly recommend that you add its base code between the opening and closing `<head>` tags on every page where you will be tracking website visitor actions. Most developers add it to their website's persistent header, so it can be used on all pages.

Placing the code within your `<head>` tags reduces the chances of browsers or third-party code blocking the pixel's execution. It also executes the code sooner, increasing the chance that your visitors are tracked before they leave your page.

96. Rush installed the Facebook Tracking Pixel to personally identify patients who click to log-in to Rush's patient portal at www.rush.edu.

97. When a patient clicks the "MyChart" button at www.rush.edu, Rush uses the patient's personal identifiers by causing the identifiers to be transmitted to Facebook attached to the fact that the patient has exchanged a communication to log-in to the My Chart patient portal:



QueryString

Name	Value
cd[buttonFeatures]	{"classList":"button-my-chart-login external","destination":"https://mychart.rush.edu/?_ga=[redacted]"_ga[redacted] to-MyChart","numChildButtons":0,"tag":"a","type":null,"name":""}
cd[buttonText]	Login to MyChart
cd[formFeatures]	[{"id":"edit-back--8nWaoUjGSDQ","name":"op","tag":"input","inputType":"submit"},{"id":"","name":"form_build_id","tag":"input","inputType":"hidden"},{"id":"","name":"form_id","tag":"input","inputType":"hidden"}]
cd[pageFeatures]	{"title":"Schedule Your Medical Appointment at Rush | Rush System"}
cd[parameters]	[]
coo	false
dl	https://www.rush.edu/schedule-your-medical-appointment-rush
ec	7
es	automatic
ev	SubscribedButtonClick
fbp	fb.[redacted]
id	[redacted]
if	false
it	[redacted]
o	30
r	stable
rl	https://www.rush.edu/
rqm	GET

98. The specific identifiers that Rush uses to help Facebook acquire and record patient communications upon the My Chart Login click include the patient's IP address and cookie values, including first party cookies Rush shares with Facebook via cookie synching.

99. Each time a Rush patient, including Plaintiffs and Class members, clicked on the "MyChart" button at www.rush.edu, Rush caused the patient's personal identifiers, including the patient's IP address, to be transmitted to Facebook attached to the fact that the patient has exchanged a communication with Rush to log-in to the My Chart patient portal.

100. In addition, through the source code deployed by Rush, the cookies that it uses to help Facebook identify patients include but are not necessarily limited to cookies named: c_user, datr, fr, and fbp.

101. Each time a Rush patient, including Plaintiffs and Class members, clicked on the "MyChart" button at www.rush.edu, Rush caused the patient's personal identifiers, including the c_user, datr, fr, and fbp cookies Rush uses to help Facebook identify patients, to be transmitted to Facebook attached to the fact that the patient has exchanged a communication with Rush to log-in to the My Chart patient portal.

102. The c_user cookie is a means of identification for Facebook users. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user

account has one – and only one – unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.

103. An unskilled computer user can obtain the c_user value for any Facebook user by (1) going to the user's Facebook page, (2) right-clicking with their mouse anywhere on the background of the page, (3) selecting 'View page source,' (4) executing a control-F function for "user=" and (5) copying the number value that immediately follows "user=" in the page source code of the target Facebook user's page.

104. It is even easier to find the Facebook account associated with a c_user cookie: one simply needs to log-in to Facebook, and then type www.facebook.com/#, with # representing the c_user cookie identifier. For example, the c_user cookie value for Mark Zuckerberg is 4. Logging in to Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck.

105. The datr cookie identifies the patient's specific web browser from which the patient is sending the communication. It is an identifier that is unique to the patient's specific web browser and is therefore a means of identification for Facebook users. Facebook keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Facebook.

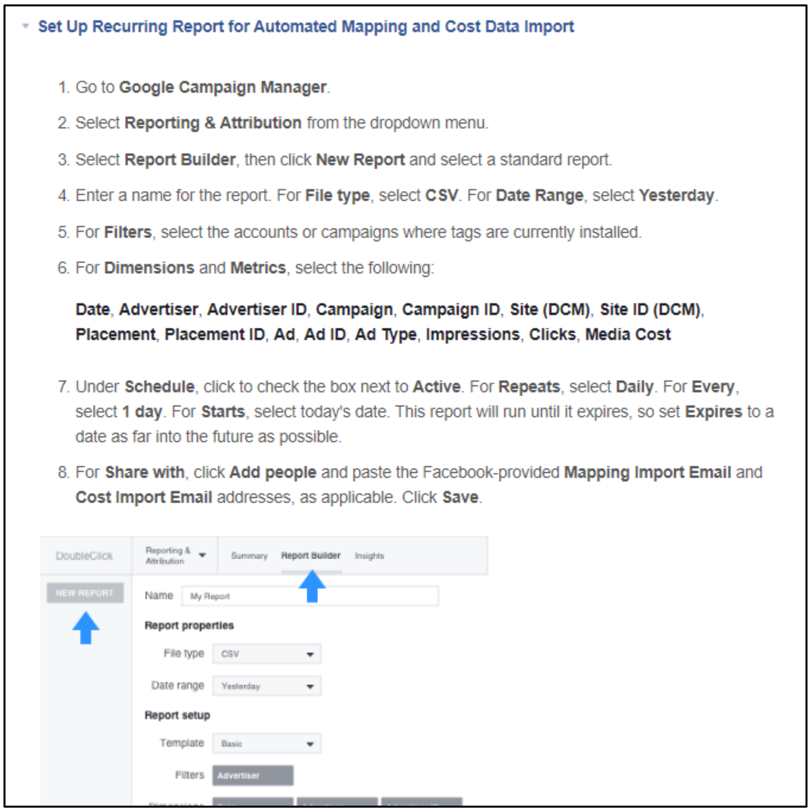
106. The fr cookie is a Facebook identifier that is an encrypted combination of the c_user and datr cookies.[15]

107. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Rush's use of the Facebook Tracking Pixel program. The fbp cookie emanates

[15] *See* Gunes Acar, Brendan Van Alsenoy, Frank Piessens, Claudia Diaz, and Bart Preneel, *Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission* (March 27, 2015) (available at https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf).

from Rush's web properties as a putative first-party cookie, but is transmitted to Facebook through cookie synching technology that hacks around the same-origin policy.

108. Facebook instructs developers on how to set-up their Google Campaign Manager to send automated regularly scheduled reports to Facebook:[16]



▾ **Set Up Recurring Report for Automated Mapping and Cost Data Import**

1. Go to **Google Campaign Manager**.
2. Select **Reporting & Attribution** from the dropdown menu.
3. Select **Report Builder**, then click **New Report** and select a standard report.
4. Enter a name for the report. For **File type**, select **CSV**. For **Date Range**, select **Yesterday**.
5. For **Filters**, select the accounts or campaigns where tags are currently installed.
6. For **Dimensions** and **Metrics**, select the following:

   Date, **Advertiser**, **Advertiser ID**, **Campaign**, **Campaign ID**, **Site (DCM)**, **Site ID (DCM)**, **Placement**, **Placement ID**, **Ad**, **Ad ID**, **Ad Type**, **Impressions**, **Clicks**, **Media Cost**

7. Under **Schedule**, click to check the box next to **Active**. For **Repeats**, select **Daily**. For **Every**, select **1 day**. For **Starts**, select today's date. This report will run until it expires, so set **Expires** to a date as far into the future as possible.
8. For **Share with**, click **Add people** and paste the Facebook-provided **Mapping Import Email** and **Cost Import Email** addresses, as applicable. Click **Save**.

Name: My Report

Report properties

File type: CSV

Date range: Yesterday

Report setup

Template: Basic

Filters: Advertiser

109. In the absence of formal discovery and access to Rush's Facebook marketing accounts, it is impossible to know whether and how much data is disclosed to Facebook through this method.

C. Bidtellect

110. Bidtellect is third-party company that operates a "programmatic platform" that collects and analyzes data to serve ads.[17]

[16] *Google Campaign Manager (DoubleClick Campaign Manager)*, Meta, https://www.facebook.com/business/help/565734646951134 (last visited July 15, 2022).

[17] *See* https://bidtellect.com/ last accessed March 28, 2023.

111. Similar to Google Analytics and Facebook Tracking Pixel, Bidtellect provides code that is embedded into the Rush web properties for tracking and analytics to provide "cookieless" tracking and retargeting solutions.[18]

112. Bidtellect's tracking connects to "bttrack.com" to measure and record user engagement and user inputs on the Rush web property sites.[19]

113. Each time a Rush patient, including Plaintiffs and Class members, clicked on the "MyChart" button at www.rush.edu, Rush caused the patient's personally identifiable patient data to be transmitted to Bidtellect attached to the fact that the patient has exchanged a communication with Rush to log-in to the My Chart patient portal.

VIII. THE INFORMATION RUSH DISCLOSES TO THIRD PARTIES IS PII AS A MATTER OF LAW

A. IP Addresses Are Personally Identifiable

114. An IP address is a number that identifies a computer connected to the Internet.

115. IP addresses are used to identify and route communications on the Internet.

116. IP addresses of individual Internet users are used by websites and tracking companies to facilitate and track Internet communications.

117. Individual homes and their occupants can be, and are, tracked and targeted with advertising using IP addresses.

118. Under the Health Insurance Portability and Accountability Act ("HIPAA"), an IP address is considered personally identifiable information. *See* 45 C.F.R. § 164.514(b)(2)(i)(O).

119. Whenever a Rush patient uses the Rush web properties, Rush uses and causes the disclosure of the patient's IP addresses to third parties with each re-directed communication

[18] *Id.*

[19] *Id.*

described herein, including patient communications about providers, conditions, treatments, appointments, bills, registration, and log-ins to the MyChart patient portal.

B. Internet Cookies Are Personally Identifiable

120. In the early years of the Internet, advertising on websites followed the same model as traditional newspapers. Just as a sporting goods store would choose to advertise in the sports section of a traditional newspaper, advertisers on the early Internet paid for ads to be placed on specific web pages based on the type of content displayed on the web page.

121. Computer programmers eventually developed "cookies"—small text files that web servers can place on a person's web browser and computing device when that person's web browser interacts with the website server. Cookies can perform different functions, like saving a user's login or other site settings. Eventually, some cookies were designed to acquire and record an individual Internet user's communications and activities on websites across the Internet.

122. Cookies are designed to and, in fact, most often do operate as a means of identification for Internet users.

123. Cookies are protected personal identifiers under HIPAA. *See* 45 C.F.R. § 164.514(b)(2)(i)(H), (J), (M), (N), and (R).

124. In general, cookies are categorized by (1) duration and (2) party.

125. There are two types of cookies classified by duration:

a. "Session cookies" are placed on a user's computing device only while the user is navigating the website that placed and accesses the cookie. The user's web browser typically deletes session cookies when the user closes the browser.

b. "Persistent cookies" are designed to survive beyond a single Internet-browsing session. The party creating the persistent cookie determines its lifespan. As a result, a persistent cookie can acquire and record a user's Internet communications for years and over dozens or hundreds of websites. Persistent cookies are sometimes called "tracking cookies."

126. Cookies are also classified by the party that uses the collected data.

a. "First-party cookies" are set on a user's device by the website with which the user is exchanging communications. For example, Rush sets a collection of its own cookies on patients' browsers when they visit any webpage on Rush's web properties. First-party cookies can be helpful to the user, server, and/or website to assist with security, log in, and functionality.

b. "Third-party cookies" are set on a user's device by website servers other than the website or server with which the user is exchanging communications. For example, the same patient who visits www.rush.edu will also have cookies on their device from third parties, such as Facebook. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies are typically used for data collection, behavioral profiling, and targeted advertising.

127. Data companies like Facebook have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell advertising that is customized to that person's communications and habits. To build individual profiles of Internet users, third party data companies assign each user a unique, or a set of unique identifiers to each user.

128. Traditionally, first- and third-party cookies were kept separate. An Internet security policy known as the same-origin policy required web browsers to prevent one web server from

accessing the cookies of a separate web server. For example, although Rush can deploy source code that uses Facebook third-party cookies to help Facebook acquire and record the patient's communications, it is not permitted direct access to Facebook third-party cookie values. The reverse was also true: Facebook was not provided direct access to the values associated with first-party cookies set by Rush.

129. Data companies have designed a way to hack around the same-origin policy so that third-party data companies gain access to first-party cookies.

130. Javascript source code developed by third-party data companies and placed on a webpage by a developer such as Rush can bypass the same-origin policy to send a first-party cookie value in a tracking pixel to the third-party data company. This technique is known as "cookie synching," and it allows two cooperating websites to learn each other's cookie identification numbers for the same user. Once the cookie synching operation is completed, the two websites can exchange any information they have collected and recorded about a user that is associated with a cookie identification number. The technique can also be used to track an individual who has chosen to deploy third-party cookie blockers.

131. Whenever a Rush patient uses the Rush web properties, Rush uses and causes the disclosure of patient cookie identifiers with each re-directed communication described herein, including patient communications about providers, conditions, treatments, appointments, bills, registration, and log-ins to the MyChart patient portal.

132. Rush's cookie disclosures include the deployment of cookie synching techniques that cause the disclosure of the first-party cookie values that Rush assigns to patients to be made to third parties.

C. Browser-Fingerprints Are Personally Identifiable

133. A browser-fingerprint is information collected about a computing device that can be used to identify the device.

134. A browser-fingerprint can be used to identify a device when the device's IP address is hidden, and cookies are blocked.

135. The Electronic Frontier Foundation has explained:

> When a site you visit uses browser fingerprinting, it can learn enough information about your browser to uniquely distinguish you from all the other visitors to that site. Browser fingerprinting can be used to track users just as cookies do, but using much more subtle and hard-to-control techniques. In a paper EFF released in 2010, we found that a majority of users' browsers were uniquely identifiable given existing fingerprinting techniques. Those techniques have only gotten more complex and obscure in the intervening years. By using browser fingerprinting to piece together information about your browser and your actions online, trackers can covertly identify users over time, track them across websites, and building an advertising profile of them.[20]

136. In 2017, researchers showed that browser fingerprinting techniques can successfully identify 99.24 percent of users.[21]

137. Browser-fingerprints are protected personal identifiers under HIPAA. *See* 45 C.F.R. § 164.514(b)(2)(i)(M), (R).

138. Whenever a Rush patient uses the Rush web properties, Rush uses and causes the disclosure of data sufficient to form a browser-fingerprint with each re-directed communication described herein, including patient communications about providers, conditions, treatments, appointments, bills, registration, and log-ins to the MyChart patient portal.

[20] Katarzyna Szymielewicz and Bill Dudington, *The GDPR and Browser Fingerprinting: How It Changes the Game for the Sneakiest Web Trackers*, Electronic Frontier Foundation (June 19, 2018) (available at https://www.eff.org/deeplinks/2018/06/gdpr-and-browser-fingerprinting-how-it-changes-game-sneakiest-web-trackers).

[21] Yinzhi Cao, Song Li and Erik Wijmans, *(Cross-)Browser Fingerprinting via OS and Hardware Level Features*, Proceedings of the Network and Distributed Security Symposium (March 2017) (available at http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf).

IX. THE PERSONALLY IDENTIFIABLE DATA AND COMMUNICATIONS RUSH USES AND DISCLOSES WITHOUT PATIENTS' KNOWLEDGE, CONSENT, AUTHORIZATION, OR FURTHER ACTION HAS VALUE

139. The value of data that companies like Facebook, Google, and Bidtellect extract from people who use the Internet is well understood and generally accepted in the e-commerce industry.

140. Personal information is now viewed as a form of currency. Professor Paul M. Schwartz noted in the Harvard Law Review:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056-57 (2004).

141. The cash value of Internet users' personal information can be quantified. In a 2015 study by the Ponemon Institute, researchers determined the value that American Internet users place on their "health condition" as more valuable than any other piece of data about them, with a minimum value of $82.90.[22]

142. Medical information derived from medical providers garners even more value from the fact that it is not available to third party data marketing companies because of strict restrictions on provider disclosures under HIPAA, state laws, and provider standards, including the Hippocratic oath.

[22] Ponemon Institute, Privacy and Security in a Connected Life: A Study of US Consumers, March 2015, available at https://vdocuments.site/privacy-and-security-in-a-connected-life-protect-personal-information-from-being.html?page=1.

143. Even with restrictions on the disclosure of personally identifiable health information, a robust market exists for the trade of de-identified health data.[23]

144. Upon information and belief, Rush was compensated for its disclosures of Plaintiffs' and Class members' personally identifiable patient data and communications by the third-party recipients in the form of enhanced marketing services or other compensation.

145. Rush did not pay or offer to pay Plaintiffs or Class members for their communications or personally-identifiable patient data associated with these disclosures before or after the disclosures were made.

146. Rush profited from Plaintiffs' and Class members' information without ever intending to compensate Plaintiffs and Class members or inform them that the disclosures had been made.

147. Rush was unjustly enriched by their conduct.

X. RUSH'S DUTIES OF CONFIDENTIALITY

A. Duties Under Federal Law

i. The HIPAA Privacy Rule protects patient health care information.

148. Patient health care information in the United States is protected by federal law under HIPAA and its implementing regulations, which are promulgated by the HHS.

149. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually

[23] *See* Adam Tanner*, How Data Brokers Make Money Off Your Medical Records,* Scientific American, https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/ (February 1, 2016); Sam Thielman, *Your Private Medical Data is for Sale – and It's Driving a Business Worth Billions*, The Guardian, https://www.theguardian.com/technology/2017/jan/10/medical-data-multibillion-dollar-business-report-warns (January 10, 2017); Adam Tanner, *The Hidden Global Trade in Patient Medical Data,* YaleGlobal Online, https://archive-yaleglobal.yale.edu/content/hidden-global-trade-patient-medical-data (last visited July 15, 2022).

identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[24]

150. The Privacy Rule broadly defines "protected health information" ("PHI") as "individually identifiable health information" ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

151. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

152. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination'"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed:

A. Names;

***

[24] HHS.gov, *Health Information Privacy* (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

> H. Medical record numbers;
>
> ***
>
> J. Account numbers;
>
> ***
>
> M. Device identifiers and serial numbers;
>
> N. Web Universal Resource Locators (URLs);
>
> O. Internet Protocol (IP) address numbers; … and
>
> R. Any other unique identifying number, characteristic, or code…; and"
>
> the covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

45 C.F.R. § 164.514.

153. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

154. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320d-6.

155. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Rush when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

156. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall "be fined not more than $250,000, imprisoned not more than 10 years, or both."

ii. Patient status is among the health information protected by HIPAA

157. An individual's status as a patient of a health care provider is protected by HIPAA. *In re Meta Pixel Healthcare Lit.*, Case No. 3:22-cv-03580-WHO, Dkt. 159 at 12, (N.D.Cal. Dec. 22, 2022) ("I agree that the information at issue here appears to show patient status and thus constitutes protected health information under HIPAA."), *Id.* at 15 ("[T]he Pixel captures information that connects a particular user to a particular health care provider—i.e., patient status—which falls within the ambit of information protected under HIPAA").

158. Guidance from HHS confirms that patient status is protected by HIPAA:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data. … **If such information was listed with health condition, health care provision** or payment data, **such as an indication that the individual was treated at a certain clinic**, then this information would be PHI.[25]

159. HHS's guidance for marketing communications states that health care providers may not provide patient lists for marketing purposes without the consent of every included patient:

[25] Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* at 5 (emphasis added) (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, **covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list**.[26]

160. HHS has instructed for decades that patient status is protected by the HIPAA Privacy Rule:

a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);

b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002);

c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013); and

d. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

iii. There is no HIPAA exception for marketing on the Internet.

161. HHS issued a bulletin in December 2022 (the "Bulletin") "to highlight the obligations" of health care providers and their business associates under the HIPAA Privacy Rule "when using online tracking technologies" such as the "Meta Pixel," which "collect and analyze

[26] Office for Civil Rights, *Marketing* at 1-2 (emphasis added) (Apr. 3, 2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.

information about how internet users are interacting with a regulated entity's website or mobile application."[27]

162. In the Bulletin, HHS reminded covered entities that HIPAA applies to health care providers' use of tracking technologies like the Meta Pixel.[28] Among other things, HHS explained that health care providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information (like an IP address) even if no treatment information is included and even if the individual does not have a relationship with the health care provider:

> How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
>
> Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website or mobile app, including individually identifiable health information (IIHI) that the individual providers when they use regulated entities' websites or mobile apps. This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. **This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.* it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care**.[29]

163. HHS explained that tracking technologies on health care providers' patient portals "generally have access to PHI" and may access diagnosis and treatment information, in addition to other sensitive data:

[27] HHS.gov, *HHS Office of Civil Rights Issue Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information* (Dec. 1, 2022), https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html.

[28] HHS.gov, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[29] *Id*. (emphasis added).

> Tracking on user-authenticated webpages
>
> Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. **Tracking technologies on a regulated entity's user-authenticated webpages generally have access to PHI.** Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. **Tracking technologies within user-authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal**. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to **only** use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.[30]

164. Tracking technology vendors like Facebook and Google are considered business associates under HIPAA if they provide services to Rush and receive or maintain PHI, as they do:

> Furthermore, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (*e.g.* health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules. For example, if an individual makes an appointment through the website of a covered health clinic for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.[31]

165. HIPAA applies to Rush's webpages with tracking technologies *even outside the patient portal*:

> Tracking on unauthenticated webpages
>
> [T]racking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of

[30] *Id*. (emphasis added).
[31] *Id*.

> unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal … **[and pages] that address[] specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances**. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.[32]

166. And no PHI may be disclosed to tracking technology vendors like Facebook and Google unless Rush has properly notified its website users and entered into a business associate agreement with the vendor:

> Regulated entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use. However, the Privacy Rule does **not** permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI.
>
> If there is not an applicable Privacy Rule permission or if the vendor is not a business associate of the regulated entity, then the individual's HIPAA-compliant authorizations are required **before** the PHI is disclosed to the vendor. Website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do **not** constitute a valid HIPAA authorization.
>
> [I]t is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.[33]

iv. The HHS Bulletin Was a Reminder to Covered Entities, Like Rush, of Existing Duties—Not a Proclamation of New Policy.

[32] *Id*. (emphasis added).

[33] *Id*.

167. HHS's bulletin did not create any new obligations or duties. Instead, it reminded covered entities of long-standing obligations with citations to existing guidance and rules that have been in place for decades.

168. The Bulletin's first sentence explains that its purpose is "to highlight the obligation of [HIPAA]-covered entities and business associates … under the HIPAA [Privacy Rules] when using online tracking technologies[.]"[34]

169. The Bulletin notes that "it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors," then explains how online tracking technologies violate the same HIPAA rules that have existed for decades.[35]

170. The Bulletin did not change or propose to change any existing rules – because the existing rules have long prohibited the types of conduct alleged in this Complaint and described in the bulletin.

171. For example, the Bulletin states that:

> All such [individually identifiable health information] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.,* it isindicative that the individual has received or will receive health care services or benefits from the coveredentity), and thus relates to the individual's past, present, or future health or health care or payment for care.[36]

172. To support this, the Bulletin cites "Modifications of the HIPAA [Rules], Final Rule," 78 FR 5566, 5598, *a rulemaking notice from January 25, 2013*, which stated:

> [P]rotected health information … may not necessarily include diagnosis-specific information, such as information about the treatment of an individual, and may be limited to demographic or other information not indicative of the type of health care services provided to an individual. If the information is tied to a covered entity, then it is protected health information by definition since it is indicative that the

[34] HHS.gov, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[35] *Id.*

[36] *Id.*

> individual received health care services or benefits from the covered entity, and therefore it must be protected … in accordance with the HIPAA rules.[37]

173. The 2013 explanation from HHS is consistent with all other rules and regulations.

174. In Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructed in 2012:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data. . . . If such information was listed with health condition, health care provision or payment data, *such as an indication that the individual was treated at a certain clinic*, then this information would be PHI.
>
> (emphasis added).[38]

175. In its guidance for Marketing, HHS further instructed in 2003:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. Emphasis added.[39]

176. On December 28, 2000, HHS specifically stated that "[t]he sale of a patient list to a marketing firm" is not permitted. 65 FR 82462, 82717.

[37] Available at https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf (last visited March 21, 2023).

[38] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule,* at 5, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (November 26, 2012).

[39] *Marketing*, at 1-2, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (April 3, 2003).

177. On January 25, 2013, HHS stated that, it would violate HIPAA "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 FR 5566, 5642.

178. In June 2022, HHS published guidance to consumers indicating again that their status as patients was protected when exchanging communications with covered entities, even on the Internet. In "Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet,"[40] HHS stated the following:

a. "Your health information provides insight into the personal, often-sensitive details of your life. Protecting the privacy and security of this information, including what doctors you visit and what medical treatments or services you receive, allows you to control who has access to information about you, how much access they have, and when they have access. This enables you to protect yourself from potential discrimination, identity theft, or harm to your reputation."

b. "The Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules protect the privacy and security of your medical and other health information when it is transmitted or maintained by covered entities (health plans, most health care providers, health care clearinghouses) and business associates (people and companies that provide certain services for covered entities). This information is referred to as protected health information (PHI), and it includes individually identifying information, such as your name, address, age, social security number, and

[40] Available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html (last visited March 21, 2023).

location, *as well as* information about your health history, any diagnoses or conditions, current health status, and more."

c. "The HIPAA Rules apply only when PHI is created, received, maintained or transmitted by covered entities and business associates."

d. "[U]nless the app is provided to you by a covered entity or its business associate, the HIPAA Rules also do not protect the privacy of data you've downloaded or entered into mobile apps for your personal use, regardless of where the information came from."

179. The underlined language "unless the app is provided to you by a covered entity or its business associate" is a hyperlink to *HHS Guidance published in 2016, titled Health App Use Scenarios & HIPAA*, which is available at: https://www.hhs.gov/sites/default/files/ocr-health-app-developer-scenarios-2-2016.pdf.

180. This 2016 guidance from HHS specifies that:

a. "If you work for [a covered entity], and as part of your job you are creating an app that involves the use or disclosure of identifiable health information, the entity … must protect that information in compliance with the HIPAA Rules. For extensive information on the requirements of the HIPAA rules and how to comply with them, please see http://www.hhs.gov/hipaa/index.html."

b. "In all cases in which a covered entity is transmitted PHI, either itself or using a business associate, it must apply reasonable safeguards to protect the information[.]"

v. HIPAA Only Contains a Single Exception for Disclosure of Patient Status Without Express Pre-Authorization, and Even Then, Patients May Opt-Out

181. Under 45 CFR § 154.510(a)(1), a covered entity may disclose a patient's name, location in the facility, condition in "general terms," and religious affiliation to (A) members of the clergy or (B) other persons who ask for the individual by name.

182. Before providing a patient's name and location in the facility, the covered entity "must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information … and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by" 45 C.F.R. § 154.510(a)(1).

vi. Disclosures for Marketing or Sales Purposes Require Special Authorization

183. Under 45 CFR § 164.508(a)(3), "a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of: (A) a face-to-face communication made by a covered entity to an individual; or (B) a promotional gift of nominal value provided by the covered entity."

184. Under 45 CFR § 164.508(a)(4), "a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart [and] [s]uch authorization must state that the disclosure will result in remuneration to the covered entity."

185. Under 45 CFR § 164.501, "marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service."

186. Under 45 CFR § 164.501, “financial remuneration” is defined as “direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payments does not include any payment for treatment of an individual.”

187. Under 45 CFR § 164.501 “treatment means the provision [or] management of health care and related services by one or more health care providers[.]”

vii. Floor Preemption: HIPAA Pre-empts All Weaker State Laws

188. HIPAA expressly preempts all State laws that are contrary to the HIPAA rules except where “[t]he provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirements, or implementation specification adopted under [HIPAA].” 45 C.F.R. § 160.203(b).

189. Other exceptions to pre-emption apply where either (1) the secretary of HHS makes a determination that the state law is necessary for certain express purposes; (2) provides for reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation or intervention; or (3) requires a health plan to provide information for the purpose of audits or the license or certification of facilities or individuals.

190. The Secretary of HHS has not issued a determination that any Illinois or other state law that does not protect patient-status is necessary for any of the purposes listed in 45 C.F.R. § 160.203.

191. To the extent this Court determines that Illinois standards, requirements, and specifications regarding whether patient-status is protected is less stringent than HIPAA standards, then that Illinois standard, requirement, or specification is expressly preempted by HIPAA.

B. Ancient and Modern Industry Standards of Patient Confidentiality

192. A medical provider’s duty of confidentiality to patients is ancient in origin.

193. The original Hippocratic Oath, circa 400 B.C., provided that physicians must pledge, "What I may see or hear in the course of treatment or even outside of the treatment in regard to the life of man, which on no account must be spread abroad, I will keep to myself holding such things shameful to be spoken about."[41]

194. The modern Hippocratic Oath provides, "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know."[42]

195. A medical provider's duty of confidentiality to patients still applies today. In fact, the American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

196. AMA Code of Medical Ethics Opinion 3.2.1 provides:

> Patients need to be able to trust that physicians will protect information shared in confidence. They should feel free to fully disclose sensitive personal information to enable their physician to most effectively provide needed services. Physicians in turn have an ethical obligation to preserve the confidentiality of information gathered in association with the care of the patient.
>
> In general, patients are entitled to decide whether and to whom their personal health information is disclosed.[43]

197. AMA Code of Medical Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care. However, respecting patient privacy in other forms is also fundamental, as an expression of respect for patient autonomy and a prerequisite for trust. Patient privacy encompasses a number of aspects, including … personal data (informational privacy)[.] . . . *Physicians must seek to protect patient privacy in all settings to the greatest extent possible* and should: (a) Minimize intrusion on privacy when the patient's privacy must be balanced against other factors. (b) Inform the patient when there has been a significant infringement on privacy of which the patient would otherwise not be aware. [and] (c) Be mindful that

[41] As recited in *Brandt v. Medical Defense Associates*, 856 S.W.2d 667, 671, n. 1 (Mo. 1993)

[42] LOUIS LASAGNE, HIPPOCRATIC OATH—MODERN VERSION, *at* http://www.pbs.org/wgbh/nova/doctors/oath_modern.html.

[43] *Code of Medical Ethics Opinion 3.2.1*, AMA, https://www.ama-assn.org/delivering-care/ethics/confidentiality (last visited September 23, 2022).

> individual patients may have special concerns about privacy in any or all of these areas.[44]

198. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of a patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information to third parties for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity) about the purpose(s) for which access would be granted.[45]

199. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> *Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored.* Physicians who collect or store patient information electronically . . . must: . . . (c) release patient information only in keeping with ethics guidelines for confidentiality.

(emphasis added).[46]

C. Consumer Expectations of Patient Privacy

i. Confidentiality is a cardinal rule of the provider-patient relationship

200. Patients are aware of their medical provider's duty of confidentiality, and, as a result, have an objectively reasonable expectation that their health care providers will not share their personally identifiable data and communications with third parties in the absence of authorization for any purpose that is not directly related or beneficial to the patient's care.

[44] *Code of Medical Ethics Opinion 3.1.1*, AMA, https://www.ama-assn.org/delivering-care/ethics/privacy-health-care (last visited September 23, 2022).
[45] *Code of Medical Ethics Opinion 3.2.4*, AMA, https://www.ama-assn.org/delivering-care/ethics/access-medical-records-data-collection-companies (last visited July 15, 2022).
[46] *Code of Medical Ethics Opinion 3.3.2*, AMA, Conf https://www.ama-assn.org/delivering-care/ethics/confidentiality-electronic-medical-records (last visited July 15, 2022).

201. A recent national survey from CVS-Aetna revealed that "[p]rivacy and data security lead patients' concerns in the changing health environment." Eighty percent of survey respondents "indicated that privacy was a top concern regarding their health care, while 76 percent of individuals felt the same high level of concern for their data security." Both totals are higher than the 73 percent of consumer who indicate that cost is important to their care.

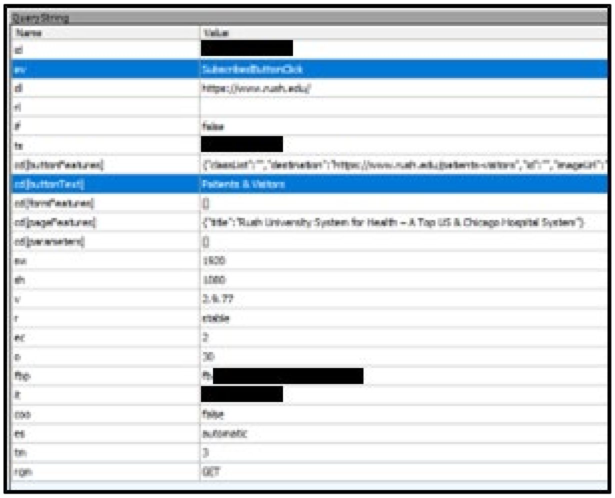
ii. Rush assures patients that it protects their personally identifiable information

202. Patients', including Plaintiffs' and Class members', reasonable expectations of privacy are further supported by express and implied promises by Rush.

iii. The Rush HIPAA Privacy Notice applies to patient communications

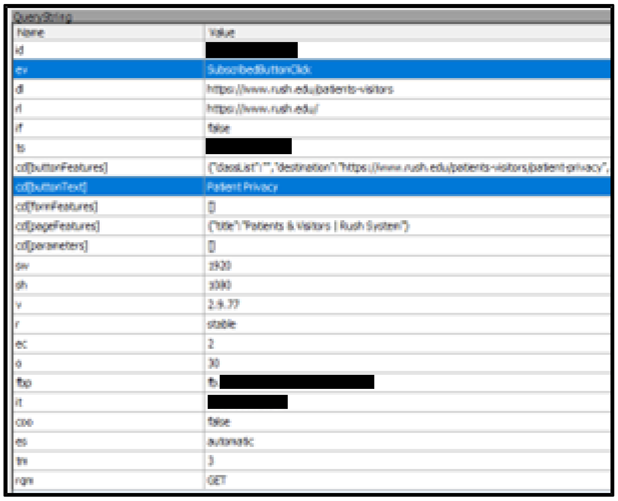
203. To comply with the requirement of posting the HIPAA notice on its web properties, Rush posts its HIPAA Notice on the Rush web properties.

204. To find the HIPAA policy, patients must navigate from the homepage to the "Patients & Visitors" tab, click on the "*Patient Privacy*" button, then click on the correct facility (*e.g.* Rush University Medical Center or Rush Oak Park Hospital), and then click on the "Notice of Privacy Practices" link. However, unbeknownst to the patient, these *patient privacy-related steps* were all being contemporaneously transmitted to Facebook and Google:



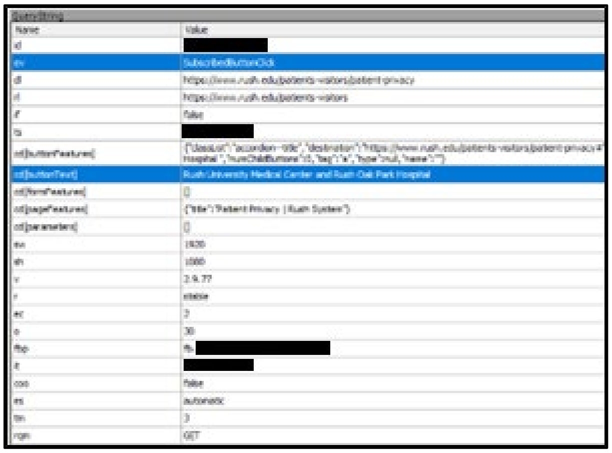
QueryString

Name	Value
id	[redacted]
ev	SubscribedButtonClick
dl	https://www.rush.edu/
rl	
if	false
ts	[redacted]
cd[buttonFeatures]	{"classList":"","destination":"https://www.rush.edu/patients-visitors","id":"","imageUrl":"
cd[buttonText]	Patients & Visitors
cd[formFeatures]	[]
cd[pageFeatures]	{"title":"Rush University System for Health – A Top US & Chicago Hospital System"}
cd[parameters]	[]
sw	1920
sh	1080
v	2.9.77
r	stable
ec	2
o	30
fbp	fb.[redacted]
it	[redacted]
coo	false
es	automatic
tm	3
rqm	GET



QueryString

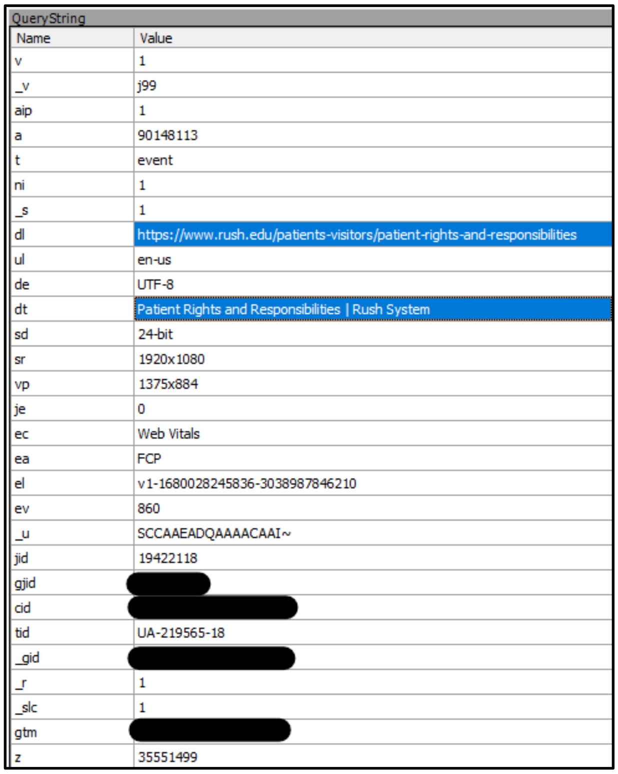
Name	Value
id	[redacted]
ev	SubscribedButtonClick
dl	https://www.rush.edu/patients-visitors
rl	https://www.rush.edu/
if	false
ts	[redacted]
cd[buttonFeatures]	{"classList":"","destination":"https://www.rush.edu/patients-visitors/patient-privacy",
cd[buttonText]	Patient Privacy
cd[formFeatures]	[]
cd[pageFeatures]	{"title":"Patients & Visitors | Rush System"}
cd[parameters]	[]
sw	1920
sh	1080
v	2.9.77
r	stable
ec	2
o	30
fbp	fb.[redacted]
it	[redacted]
coo	false
es	automatic
tm	3
rqm	GET



QueryString

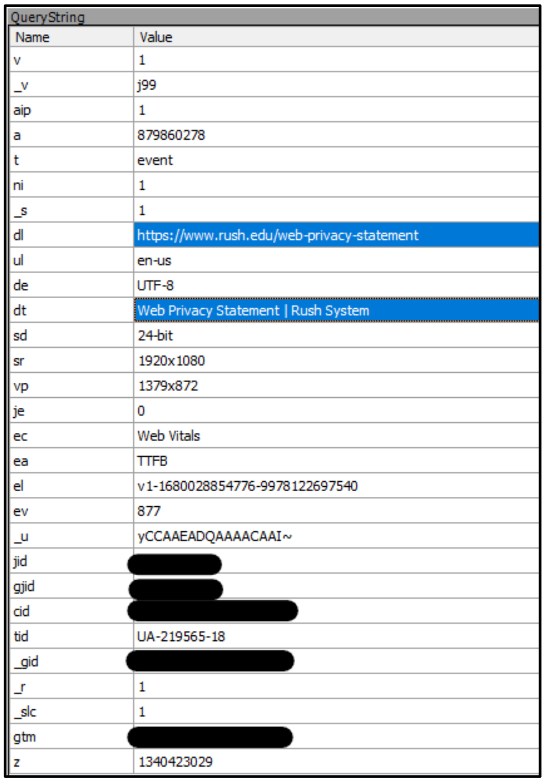
Name	Value
id	[redacted]
ev	SubscribedButtonClick
dl	https://www.rush.edu/patients-visitors/patient-privacy
rl	https://www.rush.edu/patients-visitors
if	false
ts	[redacted]
cd[buttonFeatures]	{"classList":"accordion--title","destination":"https://www.rush.edu/patients-visitors/patient-privacy# hospital","numChildButtons":0,"tag":"a","type":null,"name":""}
cd[buttonText]	Rush University Medical Center and Rush Oak Park Hospital
cd[formFeatures]	[]
cd[pageFeatures]	{"title":"Patient Privacy | Rush System"}
cd[parameters]	[]
sw	1920
sh	1080
v	2.9.77
r	stable
ec	3
o	30
fbp	fb.[redacted]
it	[redacted]
coo	false
es	automatic
tm	3
rqm	GET

205. Alternatively, patients can navigate to mychart.rush.edu, then click on the "Terms and Conditions" hyperlink, then scroll down to the section titled "I. Privacy," which instructs patients to "Please review your notice of Privacy Practices under the Related Topics area below for a thorough description of how Rush, Rush Copley and their affiliates gather, uses and protects your confidential health information," then click on the appropriate "Notice of Privacy Practices" link. Unbeknownst to the patient, these *patient privacy-related steps* were all being contemporaneously transmitted to Facebook and Google:



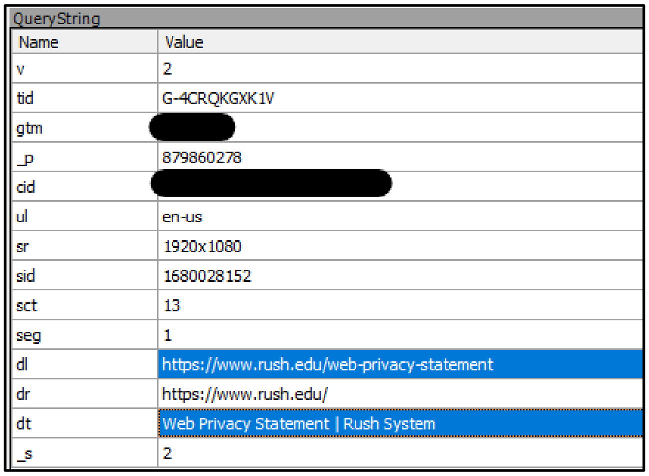
QueryString

Name	Value
v	1
_v	j99
aip	1
a	90148113
t	event
ni	1
_s	1
dl	https://www.rush.edu/patients-visitors/patient-rights-and-responsibilities
ul	en-us
de	UTF-8
dt	Patient Rights and Responsibilities | Rush System
sd	24-bit
sr	1920x1080
vp	1375x884
je	0
ec	Web Vitals
ea	FCP
el	v1-1680028245836-3038987846210
ev	860
_u	SCCAAEADQAAAACAAI~
jid	19422118
gjid	[redacted]
cid	[redacted]
tid	UA-219565-18
_gid	[redacted]
_r	1
_slc	1
gtm	[redacted]
z	35551499



QueryString

Name	Value
v	1
_v	j99
aip	1
a	879860278
t	event
ni	1
_s	1
dl	https://www.rush.edu/web-privacy-statement
ul	en-us
de	UTF-8
dt	Web Privacy Statement | Rush System
sd	24-bit
sr	1920x1080
vp	1379x872
je	0
ec	Web Vitals
ea	TTFB
el	v1-1680028854776-9978122697540
ev	877
_u	yCCAAEADQAAAACAAI~
jid	[redacted]
gjid	[redacted]
cid	[redacted]
tid	UA-219565-18
_gid	[redacted]
_r	1
_slc	1
gtm	[redacted]
z	1340423029



QueryString

Name	Value
v	2
tid	G-4CRQKGXK1V
gtm	[redacted]
_p	879860278
cid	[redacted]
ul	en-us
sr	1920x1080
sid	1680028152
sct	13
seg	1
dl	https://www.rush.edu/web-privacy-statement
dr	https://www.rush.edu/
dt	Web Privacy Statement | Rush System
_s	2

206. The very term "Privacy Policy," in general, and as used by Rush, is deceptive. Research has consistently shown that a majority of Americans who see that a website has a "Privacy Policy" falsely believe that the company with the policy cannot disclose information about them without their consent.

207. By taking such action of linking the privacy link to the HIPAA Notice of Privacy Practices, Rush gives patients the impression that it treats their communications at its web

properties with the same confidentiality that it treats patient communications at its physical properties.

208. As a matter of law, there is no exception in HIPAA for communications between patients and providers that occur over the Internet.

209. Rush's Notice of Privacy Practices makes and breaks the following promises:

a. First, Rush states that "[t]he information privacy practices in this notice will be followed by … [a]ll departments and units of our organizations," but not all departments and units of Rush follow the Privacy Practices notice. As described herein, Rush's web properties disclose personally identifiable patient data and communications to Facebook, Google, and others – even through the Notice of Privacy Practices expressly promises otherwise.

b. Second, Rush promises, "We are required by applicable federal and state law to maintain the privacy of your medical information." This statement is true, but Rush does not maintain the privacy of such information.

c. Third, Rush promises, "We must follow the privacy practices that are described in this notice while it is in effect," but Rush does not follow the privacy practices described in the notice.

d. Fourth, Rush promises, "Other uses and disclosures of medical information not covered by this notice or the laws that apply will be made only after obtaining your written authorization as required by law." However, Rush makes use of and makes disclosures of patient medical information that are not covered by the list of such uses contained in the Notice of Privacy Practices.

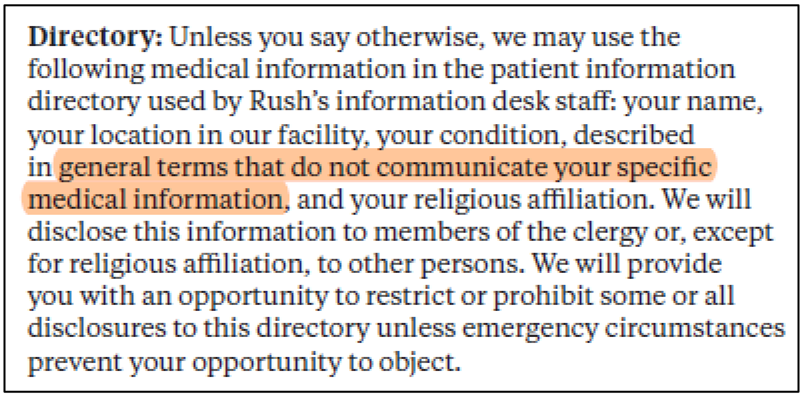
e. Fifth, Rush promises, "[W]e will not sell your medical information … without your prior written authorization," but Rush does sell medical information without prior written authorization. Specifically, Rush exchanges information regarding patients and patient communications on its web properties with Facebook, Google, and others in return for enhanced advertising and marketing services or other valuable consideration by Facebook and Google.

f. Sixth, Rush promises, "[W]e will not … use or disclose your medical information for marketing without your prior written authorization," but Rush does use and disclose patient medical information, including for marketing, without prior written authorization. Specifically, Rush uses and discloses patient information for marketing by deploying source code that collects and commands Plaintiffs' computing devices to simultaneously forward their identifiable information and the content of their communications to Facebook, Google, and others for marketing purposes.

g. Seventh, Rush promises, "Unless you give us a written authorization, we cannot use or disclose your medical information for any reason except those described in this notice." However, Rush breaks this promise as described herein.

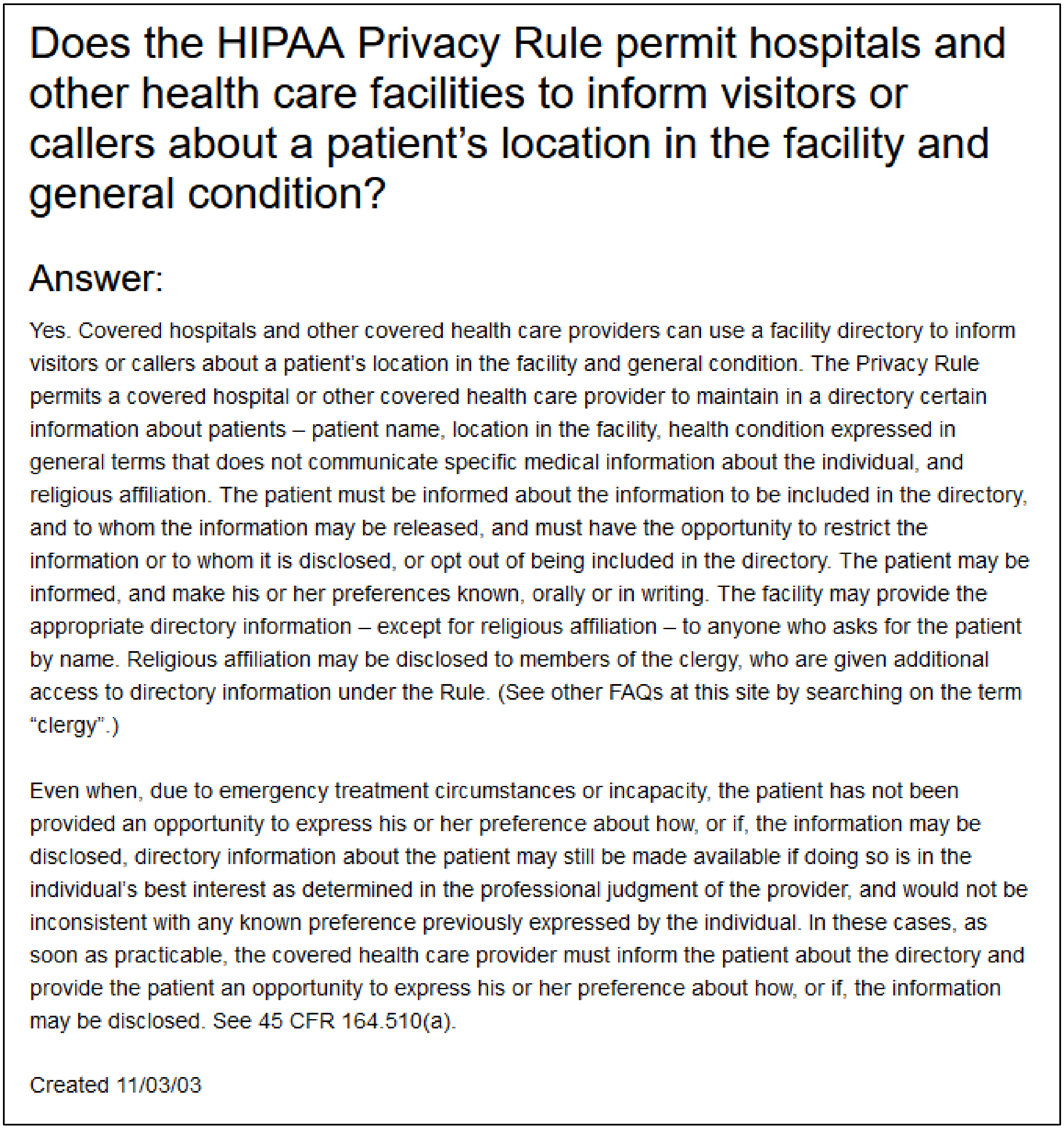
https://www.rush.edu/sites/default/files/2049-notice-privacy-11x17.pdf (last visited Mar. 6, 2023).

210. The Rush Notice of Privacy Practices also defines patient-status alone to be medical information, including disclosures without other "specific medical information." Specifically, the Notice states:



Directory: Unless you say otherwise, we may use the following medical information in the patient information directory used by Rush's information desk staff: your name, your location in our facility, your condition, described in general terms that do not communicate your specific medical information, and your religious affiliation. We will disclose this information to members of the clergy or, except for religious affiliation, to other persons. We will provide you with an opportunity to restrict or prohibit some or all disclosures to this directory unless emergency circumstances prevent your opportunity to object.

211. This identification of patient status is the only exception for disclosures completely unrelated to health or healthcare operations of which Plaintiffs' are aware in HIPAA and is consistent with 45 CFR § 164.510(a) and guidance on the HHS website since 2003:



Does the HIPAA Privacy Rule permit hospitals and other health care facilities to inform visitors or callers about a patient's location in the facility and general condition?

Answer:

Yes. Covered hospitals and other covered health care providers can use a facility directory to inform visitors or callers about a patient's location in the facility and general condition. The Privacy Rule permits a covered hospital or other covered health care provider to maintain in a directory certain information about patients – patient name, location in the facility, health condition expressed in general terms that does not communicate specific medical information about the individual, and religious affiliation. The patient must be informed about the information to be included in the directory, and to whom the information may be released, and must have the opportunity to restrict the information or to whom it is disclosed, or opt out of being included in the directory. The patient may be informed, and make his or her preferences known, orally or in writing. The facility may provide the appropriate directory information – except for religious affiliation – to anyone who asks for the patient by name. Religious affiliation may be disclosed to members of the clergy, who are given additional access to directory information under the Rule. (See other FAQs at this site by searching on the term "clergy".)

Even when, due to emergency treatment circumstances or incapacity, the patient has not been provided an opportunity to express his or her preference about how, or if, the information may be disclosed, directory information about the patient may still be made available if doing so is in the individual's best interest as determined in the professional judgment of the provider, and would not be inconsistent with any known preference previously expressed by the individual. In these cases, as soon as practicable, the covered health care provider must inform the patient about the directory and provide the patient an opportunity to express his or her preference about how, or if, the information may be disclosed. See 45 CFR 164.510(a).

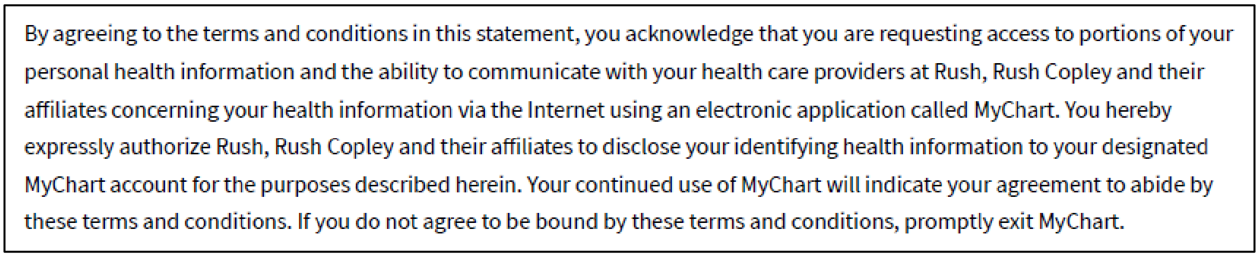
Created 11/03/03

iv. Terms and Conditions for patients who sign up for the rush mychart patient portal

212. Every patient who signs up for the Rush MyChart patient portal is subject to the Terms and Conditions that Rush applies to the relationship upon sign-up for the portal.

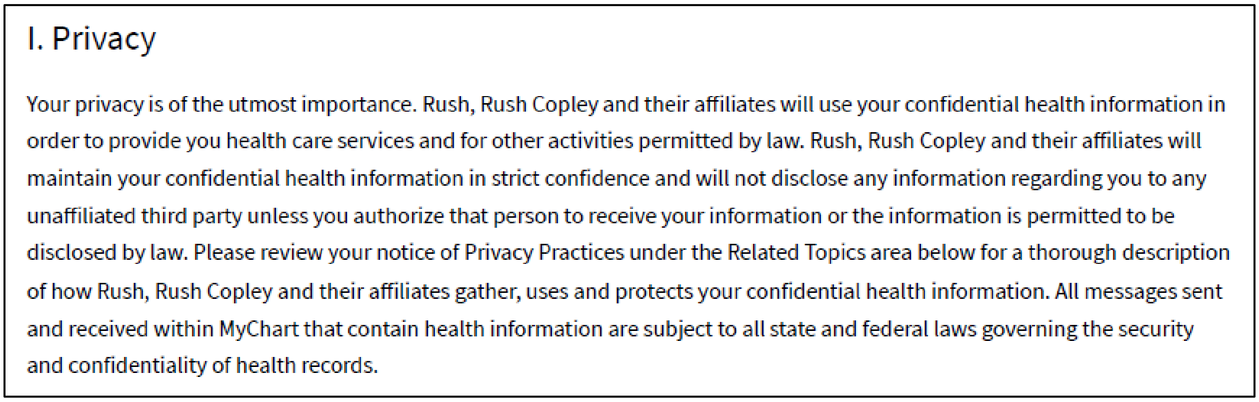
213. The Rush MyChart patient portal Terms and Conditions includes the following relevant statements and promises.

214. The Rush Terms state that:



By agreeing to the terms and conditions in this statement, you acknowledge that you are requesting access to portions of your personal health information and the ability to communicate with your health care providers at Rush, Rush Copley and their affiliates concerning your health information via the Internet using an electronic application called MyChart. You hereby expressly authorize Rush, Rush Copley and their affiliates to disclose your identifying health information to your designated MyChart account for the purposes described herein. Your continued use of MyChart will indicate your agreement to abide by these terms and conditions. If you do not agree to be bound by these terms and conditions, promptly exit MyChart.

215. The first section of the Rush Terms and Conditions states:



I. Privacy

Your privacy is of the utmost importance. Rush, Rush Copley and their affiliates will use your confidential health information in order to provide you health care services and for other activities permitted by law. Rush, Rush Copley and their affiliates will maintain your confidential health information in strict confidence and will not disclose any information regarding you to any unaffiliated third party unless you authorize that person to receive your information or the information is permitted to be disclosed by law. Please review your notice of Privacy Practices under the Related Topics area below for a thorough description of how Rush, Rush Copley and their affiliates gather, uses and protects your confidential health information. All messages sent and received within MyChart that contain health information are subject to all state and federal laws governing the security and confidentiality of health records.

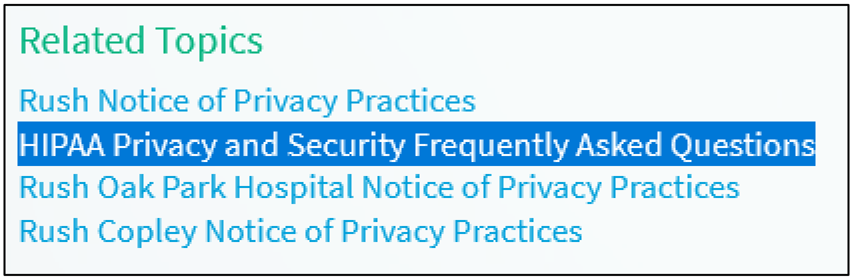
216. Rush violates these promises in several ways, including that:

a. First, although Rush promises to "maintain your confidential health information in strict confidence," it does not keep this promise. To the contrary, Rush shares patients' confidential health information with Facebook, Google, and others.

b. Second, although Rush promises that it "will not disclose any information regarding you to any unaffiliated third party unless you authorize that person to receive your information or the information is permitted to be disclosed by law," it does not keep this promise. To the contrary, Rush discloses information regarding patients to Facebook, Google, and others without authorization or legal permission.

c. Third, although Rush states that the Privacy Practices are a "thorough description of how Rush …. Gather[s], uses, and protects your confidential health information," it does not keep this promise. As described above, the HIPAA Privacy Notice documents do not disclose Rush's true activities with respect to patient privacy in their confidential health information.

d. Fourth, Rush incorporates by reference its Notice of Privacy Practices and "HIPAA Privacy and Security Frequently Asked Questions," and hyperlinks to each of these documents.



Related Topics

Rush Notice of Privacy Practices
HIPAA Privacy and Security Frequently Asked Questions
Rush Oak Park Hospital Notice of Privacy Practices
Rush Copley Notice of Privacy Practices

(highlighting added).

e. Fifth, Rush also promises that "Use of MyChart by Rush … occurs over a secure connection," but it does not keep this promise. To the contrary, Rush discloses MyChart communications to Google.

217. The HIPAA Privacy and Security Frequently Asked Questions link takes patients to the HHS website at https://www.hhs.gov/hipaa/for-professionals/faq/index.html. Among other information available through the FAQ tool, patients are told that:

a. "Doctors may not provide patient lists to [third parties] … without an authorization." According to HHS, this statement has been present since

December 19, 2002. https://www.hhs.gov/hipaa/for-individuals/faq/275/does-hipaa-expand-providers-ability-to-use-protected-health-information-for-marketing/index.html.

b. "The HIPAA Privacy Rule expressly requires an authorization for uses and disclosures of protected health information for ALL marketing communications, except in two circumstances: (1) when the communication occurs in a face-to-face encounter between the covered entity and the individual; or (2) the communication involves a promotional gift of nominal value. If the marketing communication involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved." According to HHS, this statement has been present since December 20, 2002. https://www.hhs.gov/hipaa/for-professionals/faq/278/when-is-patient-authorization-required-for-marketing/index.html.

v. False and misleading statements in the ineffective rush "Web Privacy Statement"

218. A health care provider's duty of confidentiality cannot be waived via an inconspicuous, unenforceable browse-wrap privacy policy (like that used by Rush in its footer) regardless of the contents of the policy. This is especially true where the browse-wrap policy is not provided via effective notice but is only viewable if a user scrolls through multiple separate screens of content, and then is displayed on an in descript black footer on an otherwise white page.

219. In the absence of effective notice, browse-wrap statements do not create enforceable contracts against consumers.

220. The vast majority of Internet users do not read privacy policies or website terms of use. One study found that only between 0.05 to 0.22 percent of online shoppers (or 1 to 2 of every 1,000 shoppers) access online agreements—even click- or scroll-wrap agreements rather than browse-wrap agreements.

221. Chief Justice John Roberts admits he does not read purported online agreements.

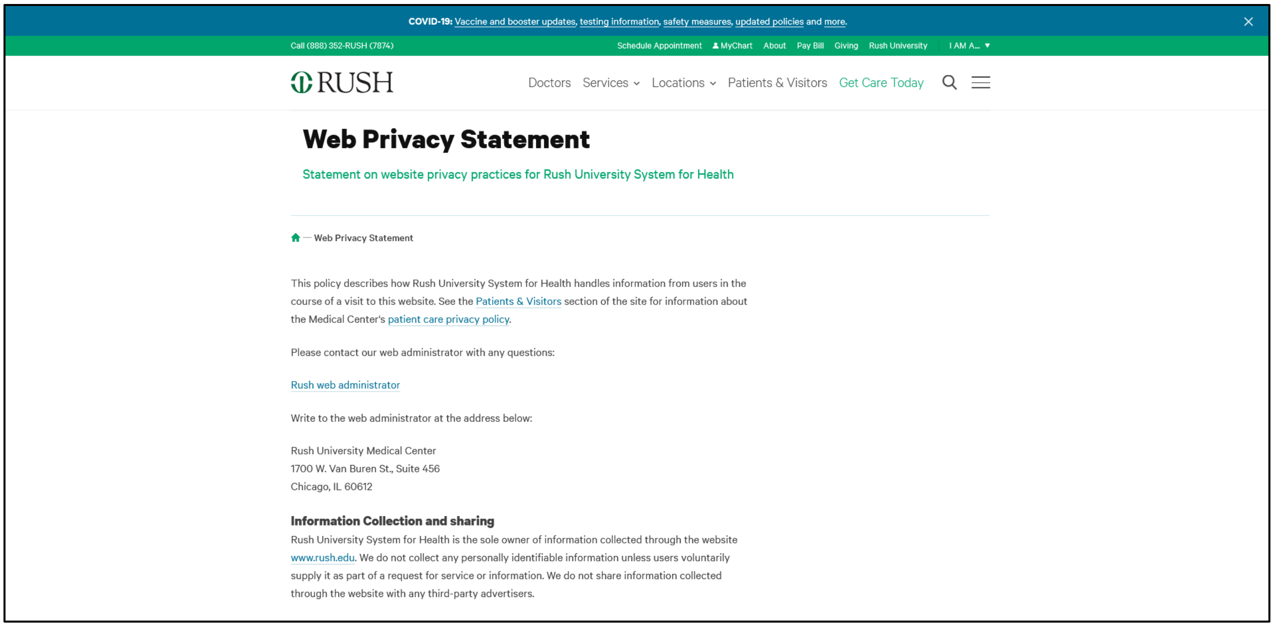
222. The cost of reading all privacy policies a consumer encounters is high. It would take an average American consumer between 181 to 304 hours per year to read the purported privacy policies of websites with which they interact. This would require a consumer to devote an estimated 40 minutes per day to reading privacy policies. The time-money calculation for this effort is between $2,553 to $5,038 per year per consumer for a collective national cost of $559.7 billion to $1.1 trillion per year.

223. Regardless, it is reasonable for a patient to assume that their health care providers' privacy policies are consistent with their providers' duties of confidentiality and patient expectations of privacy.

224. HHS has made clear that a health care provider cannot meet its privacy disclosure obligations under federal law through a website privacy statement.

225. Nothing in the Rush HIPAA Privacy Notice or MyChart patient portal Terms and Conditions apprises patients that their personal information is treated differently than as described in the HIPAA Privacy Notice or MyChart patient portal Terms and Conditions.

226. The footer on the Rush web properties also includes a hyperlink for "Web Privacy Statement," which sends the patient to a page titled "Web Privacy Statement":



Web Privacy Statement

Statement on website privacy practices for Rush University System for Health

— Web Privacy Statement

This policy describes how Rush University System for Health handles information from users in the course of a visit to this website. See the Patients & Visitors section of the site for information about the Medical Center's patient care privacy policy.

Please contact our web administrator with any questions:

Rush web administrator

Write to the web administrator at the address below:

Rush University Medical Center
1700 W. Van Buren St., Suite 456
Chicago, IL 60612

Information Collection and sharing

Rush University System for Health is the sole owner of information collected through the website www.rush.edu. We do not collect any personally identifiable information unless users voluntarily supply it as part of a request for service or information. We do not share information collected through the website with any third-party advertisers.

https://www.rush.edu/web-privacy-statement (last visited Aug. 26, 2022).

227. Even if a "Web Privacy Statement" could be effective, the Rush Web Privacy Statement makes at least ten misstatements, misrepresentations, or omissions of material fact.

228. First, Rush asserts that it "is the sole owner of information collected through the website www.rush.edu." This statement is false and misleading in that it suggests that Rush is the only entity collecting information through www.rush.edu and omits that Facebook, Google, and others are able to collect information about patients at www.rush.edu because Rush has chosen to deploy source code from those companies that command patient communications devices to contemporaneously re-direct patient information and the content of patient communications to Facebook, Google, and others.

229. Second, Rush states that, "We do not collect any personally identifiable information unless users voluntarily supply it as part of a request for service or information." This statement is false and misleading in that it suggests that personally identifiable information is not collected through Rush's web properties and omits that Facebook, Google, and others receive personally identifiable information about Rush patients when they visit www.rush.edu, mychart.rush.edu, and

Rush's MyChart patient portal because Rush has chosen to deploy source code from those companies that command patient communications devices to contemporaneously re-direct patient information and the content of patient communications to Facebook, Google, and others.

230. Third, Rush states, "We do not share information collected through the website with any third-party advertisers." This statement is false and misleading in that Rush does share information collected through its web properties with Facebook, Google, and others.

231. Fourth, Rush states that "A 'cookie' is a small file that a website puts on a user's computer with their agreement." This statement is false and misleading in that patient Class members' did not consent to the placement of any third-party cookies on their computing devices for use in connection with their communications exchanged with Rush.

232. Fifth, Rush states that, "This website uses cookies to track how visitors use the website. Cookies also streamline a user's experience of the website during a visit." These statements are misleading and irrelevant because stating that "This website uses cookies to track" implies that Rush is doing the tracking, whereas Rush omits that it uses cookies at the Rush web properties that provide confidential patient information to Facebook, Google, and others in connection with marketing. Rush's later statement about Google Analytics is not sufficient for the reason stated below.

233. Sixth, Rush states that, "In most cases, a web browser will automatically accept cookies. Users should be able to change browser settings to disable cookies. Disabling cookies may make it more difficult to use some parts of the website. For more information about deleting cookies, see the web browser's help section." These statements are false and misleading because, if a patient seeks to use the Rush patient portal, their browser must be set to accept first-party cookies, and, as a result of that, Rush will deposit cookies from Facebook and Google (third-

parties) that are disguised as first-party cookies. Thus, patients who exchange communications with Rush via its web properties are not "able to change browser settings to disable cookies" and still use the patient portal.

234. Seventh, Rush states, "Like many websites, www.rush.edu uses Google Analytics to gather information about how visitors use the website. Users may opt out if they do not want their data to be used by Google Analytics. Visit Google to learn more." This statement is false and misleading in that: (1) it omits the material fact that Rush uses Google Analytics for marketing purposes; (2) it omits the material fact that Rush shares personal information about patients with Google – through Google Analytics, Google Ads, Google Doubleclick, and Google reCaptcha; (3) it omits the material fact that Rush shares personal information about patients with Google inside what Rush promises to be its "secure" patient portal; (4) it omits that the opt-out provision that Rush references does not permit users to opt-out of their information being sent to Google Analytics; and (5) it is misleading to place the statement about Google Analytics under the "cookies" section because it suggests that Google Analytics (as a service of a third-party) would operate through third-party cookies, but Google Analytics works through the placement of third-party cookies that are disguised as first-party cookies.

235. Eighth, Rush states that, "Any personally identifiable information we collect is securely stored within a database" that "use[s] standard, industry-wide procedure to protect information we receive from visitors to the website." These statements are false and misleading in that they suggest that the "personally identifiable information" Rush collects through is web properties are not shared with third parties in the absence of a patient's authorization. However, Rush has designed its web properties to automatically duplicate and re-direct patient identifiers

(including cookies, device identifiers, and IP addresses) to third parties connected to the content of patient communications with Rush.

236. Ninth, Rush states that "[t]hough Rush University makes every effort to preserve user privacy, we may need to disclose personal information when we have a good faith belief that this is necessary to comply with a judicial proceeding, court order, government investigation, or legal process served our website." These statements are false and misleading because (1) Rush does not make every effort to preserve user privacy, instead it has designed its web properties with the purpose of providing patient identifiers and the content of patient communications to Facebook, Google and others. And (2) the statement gives patients the impression that Rush will only "disclose" personal information in the circumstances specified when, in fact, Rush discloses personal information every time that a patient exchanges a communication on the Rush web properties, including the patient portal.

237. The following chart contains a list of 37 Rush misstatements, misrepresentations, or omissions in its various policies. Plaintiffs reserve the right to expand the list upon discovery.

NOTICE OF PRIVACY PRACTICES	
1	"This notice describes how medical information about you may be used and disclosed."
2	"This notice applies to all records regarding your care generated by Rush."
3	"The information privacy practices in this notice will be followed by … [a]ll departments and units of our organizations[.]"
4	"We are required by applicable federal and state law to maintain the privacy of your medical information."
5	"We must follow the privacy practices that are described in this notice while it is in effect."
6	The Privacy Notice expressly states that "medical information in the patient information directory used by Rush's state" includes patient status and "condition, described in general terms that do not communicate your specific medical information."
7	"Other uses and disclosures of medical information not covered by this notice or the laws that apply will be made only after obtaining your written authorization as required by law."
8	"[W]e will not sell your medical information … without your prior written authorization[.]"
9	"[W]e will not … use or disclose your medical information for marketing without your prior written authorization[.]"

10	“Unless you give us a written authorization, we cannot use or disclose your medical information for any reason except those described in this notice.”
11	“[W]e will request your authorization for certain marketing activities, including any activities that involve the sale of Protected Health Information.”
MYCHART PATIENT PORTAL TERMS AND CONDITIONS	
12	“Your privacy is of the utmost importance.”
13	“Rush … will maintain your confidential health information in strict confidence and will not disclose any information regarding you to any unaffiliated third party unless you authorize that person to receive your information or the information is permitted to be disclosed by law.”
14	“Please review your notice of Privacy Practices under the Related Topics area below for a thorough description of how Rush … gather[s], uses, and protects your confidential health information.”
15	The Rush Patient Portal Policy refers patients to “HIPAA Privacy and Security Frequently Asked Questions,” which links to the HHS FAQ page at https://www.hhs.gov/hipaa/for-professionals/faq/index.html, thereby incorporating HHS FAQs.
16	“Use of MyChart by Rush … occurs over a secure connection.”
17	“All of the confidential health information available to you in MyChart is protected and securely maintained.”
18	“Rush, … afford[s] the same degree of confidentiality to health information stored in MyChart as is given to health information stored by Rush, Rush Copley and their affiliates in any other medium.”
19	“Rush … [is] committed to protecting the confidentiality of this health information.”
20	“Rush … has taken steps to make all information received from our online visitors as secure as possible against unauthorized access and use.”
21	“If the URL beings with https:// (instead of http://), the document comes from a secure server. This means your data cannot be read or deciphered by unauthorized individuals.”
WEBSITE PRIVACY STATEMENT	
22	“This policy describes how Rush … handles information from users in the course of a visit to this website. See the Patients & Visitors section of the site for information about the Medical Center’s patient care privacy policy.”
23	The sentence referring patients to the “patient care privacy policy” sends patients to the Notice of Privacy Practices, thereby incorporating such notice by prominent reference and hyperlink in the “website privacy statement.” The first sentence of the page with the Notice of Privacy Practices promises, “Rush University System is committed to protecting your health information and upholding your privacy.”
24	Rush “is the sole owner of information collected through the website www.rush.edu.”
25	“We do not collect any personally identifiable information unless users voluntarily supply it as part of a request for service or information.”
26	“We do not share information collected through the website with any third-party advertisers.”
27	“A ‘cookie’ is a small file that a website puts on a user’s computer with their agreement.”
28	“This website uses cookies to track how visitors use the website.”
29	“Cookies also streamline a user’s experience of the website during a visit.”
30	“In most cases, a web browser will automatically accept cookies. Users should be able to change browser settings to disable cookies. Disabling cookies may make it more difficult to use some parts of the website. For more information about deleting cookies, see the web browser’s help section.”

31	"Like many websites, www.rush.edu uses Google Analytics to gather information about how visitors use the website. Users may opt out if they do not want their data to be used by Google Analytics. Visit Google to learn more."
32	"For information on security of communications between Rush … and patients, please see the patient privacy information on this site." (Linking to the Notice of Privacy Practices).
33	"There are secure forms on the Rush website for users to request services and information via the internet. Users may need to provide confidential health information to help Rush fulfill a request. We will use this information only to help us respond to the user's request."
34	"To prevent unauthorized access … Rush … has put in place appropriate physical, electronic, and administrative procedures to safeguard and secure the information we collect through these online forms."
35	"Any personally identifiable information we collect is securely stored within a database" that "use[s] standard, industry-wide procedure to protect information we receive from visitors to the website."
36	"Users are prohibited from violating or attempting to violate the security of this website, including, without limitation, (a) accessing data not intended for them …. (b) attempting to … breach security …without proper authorization; …. (c) accessing or using the website or any portion … without authorization, in violation of this policy or in violation of applicable law. Violations of … security may result in civil or criminal liability."
37	"Though Rush University makes every effort to preserve user privacy, we may need to disclose personal information when we have a good faith belief that this is necessary to comply with a judicial proceeding, court order, government investigation, or legal process served our website."

XI. PATIENTS HAVE PROTECTABLE PROPERTY INTERESTS IN THEIR INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

238. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things like data and communications. Plaintiffs and Class members have a vested property right in their individually identifiable health information.

239. Illinois courts have described property broadly:

a. "Property consists of certain rights in things secured by law. These rights are usually defined to be the right of user, the right of exclusion, and the right of disposition. In a strict sense, land is not property, but the subject of property." *Rigney v. City of Chicago*, 102 Ill. 64 (1881).

b. "Property is the right and interest which one has in lands and chattels to the exclusion of others. The term 'property' includes every species of valuable right and interest. Value is the price deemed or accepted as equivalent to the

> utility of anything, and compensation is that which constitutes or is regarded as an equivalent. It is impossible to conceive of a thing such as property wholly separated from the element of value. From the very term 'property' the law infers some value; and, if no value is shown, the inference will be that it is the nominal sum of one cent, one penny, or one dollar." *Illinois Cent. R. Co. v. Commissioners of Highways and Town of Mattoon*, 161 Ill. 247, 251 (1896).

240. The United States Supreme Court has explained that, "Confidential business information has long been recognized as property." *Carpenter v. United States*, 484 U.S. 19, 26 (1987). "Depriv[ation] of [the] right to exclusive use of … information" causes a loss of property "for exclusivity is an important aspect of confidential business information and most private property for that matter." *Id*. at 27. There is no doubt that Rush has a "property right" in patient data such that, if Facebook or Google took such information from Rush without authorization, Rush would have a claim for Facebook and Google's taking of their property. Patients also have a property right in their own health information that may not be taken or used by Rush without their authorization for non-health care related reasons.

241. Federal and state law grant patients the right to protect the confidentiality of data that identifies them as patients of a particular health care provider and restrict the use of their health data, including their status as a patient, to only uses related to their care or otherwise authorized by federal or state law in the absence of patient authorization.

242. A patient's right to protect the confidentiality of their health data and restrict access to it is a valuable right.

243. In addition to property rights in their health data, patients enjoy property rights in the privacy of their health communications.

244. Patient property rights in their health data and communications are established by HIPAA and state health privacy laws that are equally or more stringent than HIPAA.

245. American courts have long recognized common law property rights in the content of a person's communications that are not to be used or disclosed to others without authorization.

246. Property rights in communications and information privacy are established by:

a. The Electronic Communications Privacy Act, including Title I (the Wiretap Act); Title II (the Stored Communications Act); and Title III (the Pen Register Act);

b. State laws that establish a right to keep communications confidential; and

c. Common law information property rights regarding the exclusive use of confidential information that have existed for centuries and continue to exist. *See Folsom v. Marsh*, 9 F.Cas. 342, 346 (C.C.D. Mass. 1841) (Story, J); *Baker v. Libbie*, 210 Mass. 599, 602 (1912); *Denis v. LeClerc*, 1 Mart. (La.) 297 (1811).

247. Rush's unauthorized acquisition, use, and disclosure of Plaintiffs' and Class members' individually identifiable health information for marketing purposes violated their property rights to control how their health data and communications are used and who may be the beneficiaries of their data and communications.

XII. PLAINTIFFS DID NOT RECEIVE THE BENEFIT OF THE BARGAIN THEY HAD WITH RUSH

248. Rush does not generally provide its medical services for free. All Rush patients, including Plaintiffs, pay Rush either directly or indirectly (e.g. through insurance, which they pay for) for medical services. The fees Rush charges may be itemized to a certain degree, for example the charges may be separated by treatment or medical procedure. But even at their most itemized level, those charges cover a wide range of services that Rush is providing with respect to any given treatment. For example, patients do not receive a separate charge for the dressing gown they wear before surgery. Yet clearly that dressing gown has real value, and is part of medical services that Rush provides to a surgery patient, and therefore the fee charged for the surgery reflects the value

of that dressing gown, even though it is not separately itemized on their bill. If Rush told its patients that such items would be covered as part of their surgery, and yet Rush then made the patient separately purchase a gown in the hospital lobby before surgery, that patient clearly would not have received the benefit of the bargain struck with Rush.

249. So too, when Rush purports to provide its patients with a modern, convenient and secure means of obtaining medical services, including scheduling appointments, communicating with doctors, and obtaining test results, that is an integral part of the medical services that Rush provides, that has real value even if it is not separately itemized on the patients bill. Rush touts the convenience and privacy of such services through its MyChart patient portal and other web properties. Therefore, when Rush failed to follow through in providing the MyChart patient portal with the promised level of privacy and security, Rush patients (including Plaintiffs) did not receive the full benefit of the bargain that they struck with Rush when they paid for their medical services.

XIII. PLAINTIFFS OVERPAID FOR RUSH'S HEALTH AND PATIENT PORTAL

250. In addition to the kinds of traditional fees and payments described above, in the modern economy, consumers pay for services with more than money.

251. On the Internet, consumers often pay for services by granting the company with which they are engaged a license to collect and use their personal data for marketing purposes.

252. Although increasing in prevalence due to the Internet, there is nothing novel about such arrangements. Bartering occurred prior to the invention of currency. The exchange of a data license for use of a service is a modern-day bartering arrangement.

253. Thus, although certain services do not involve the payment of money, they are not free. Consumers pay for the services by giving a license to use their data instead.

254. The right to collect and use consumer data is valuable and monetizable—by companies and consumers. This is particularly true of health information.

255. On the surface, the price of Rush's health care services includes the payments that users made to Rush. But Rush what failed to disclose to patients is that it was also granting itself that it would also charge patients in the form of a license to collect, disclose to third-parties, and use their health information for Rush's own benefit, including for marketing purposes.

256. In signing up for the patient portal and becoming a Rush patient, Plaintiffs and Class members granted Rush a license to use their information and communications content that was limited to the purposes listed in the Rush Notice of Privacy Practices and the Rush MyChart patient portal Terms and Conditions.

257. The Rush Notice of Privacy Practices expressly promises patients that the Notice "applies to all records regarding your care generate by Rush," "will be followed by … [a]ll departments and units of our organizations," and that information that Rush receives from patients as part of its healthcare services contract will not be used for any purpose outside of those specifically listed in the Notice of Privacy Practices unless Rush "obtain[s] your written authorization as required by law." More specifically, Rush promises that it: (1) "will not sell your medical information" or (2) "use or disclose your medical information for marketing without your prior written authorization." Rush also promises that "Unless you give us a written authorization, we cannot use or disclose your medical information for any reason except those described in this notice."

258. Thus, the limits of the data license that Rush obtains in order to provide medical services to patients is prescribed by the Notice of Privacy Practices and did not include using, disclosing, or selling patient information for marketing purposes.

259. Rush overcharged patients by granting itself a license to use and disclose valuable patient health data beyond the license and limitations specifically stated in the Notice of Privacy Practices.

260. The Rush MyChart patient portal Terms and Conditions contains additional express promises that limit the data license that Rush charges and patients pay to Rush in exchange for use of the patient portal. The MyChart patient portal Terms and Conditions states (1) that Rush (1) "will maintain your confidential health information in strict confidence;" (2) that Rush "will not disclose any information regarding you to any unaffiliated third party unless you authorize that person to receive your information or the information is permitted to be disclosed by law;" (3) that "Rush … afford[s] the same degree of confidentiality to health information stored in MyChart as is given to health information stored by Rush … in any other medium; and (4) "Rush … [is] committed to protecting the confidentiality of this health information."

261. Thus, the limits of the data license that Rush obtains to provide medical services via Rush's MyChart patient portal is prescribed by the MyChart patient portal Terms and Conditions and the Notice of Privacy Practices and did not include using, disclosing, or selling patient information for marketing purposes.

262. The existence of the Website Privacy Statement did not alter the data license that Rush stated would be part of the contract for healthcare services or the patient portal.

263. The MyChart patient portal Terms and Conditions states that it "contains the entire agreement between the parties with respect to the subject matter contained herein and shall not be modified or amended except by signed written instrument."

264. The MyChart patient portal Terms and Conditions also incorporate (1) the Rush Notice of Privacy Practices; and (2) all HHS guidance on HIPAA rights by express and prominent reference and hyperlink in the text of the MyChart patient portal Terms and Conditions.

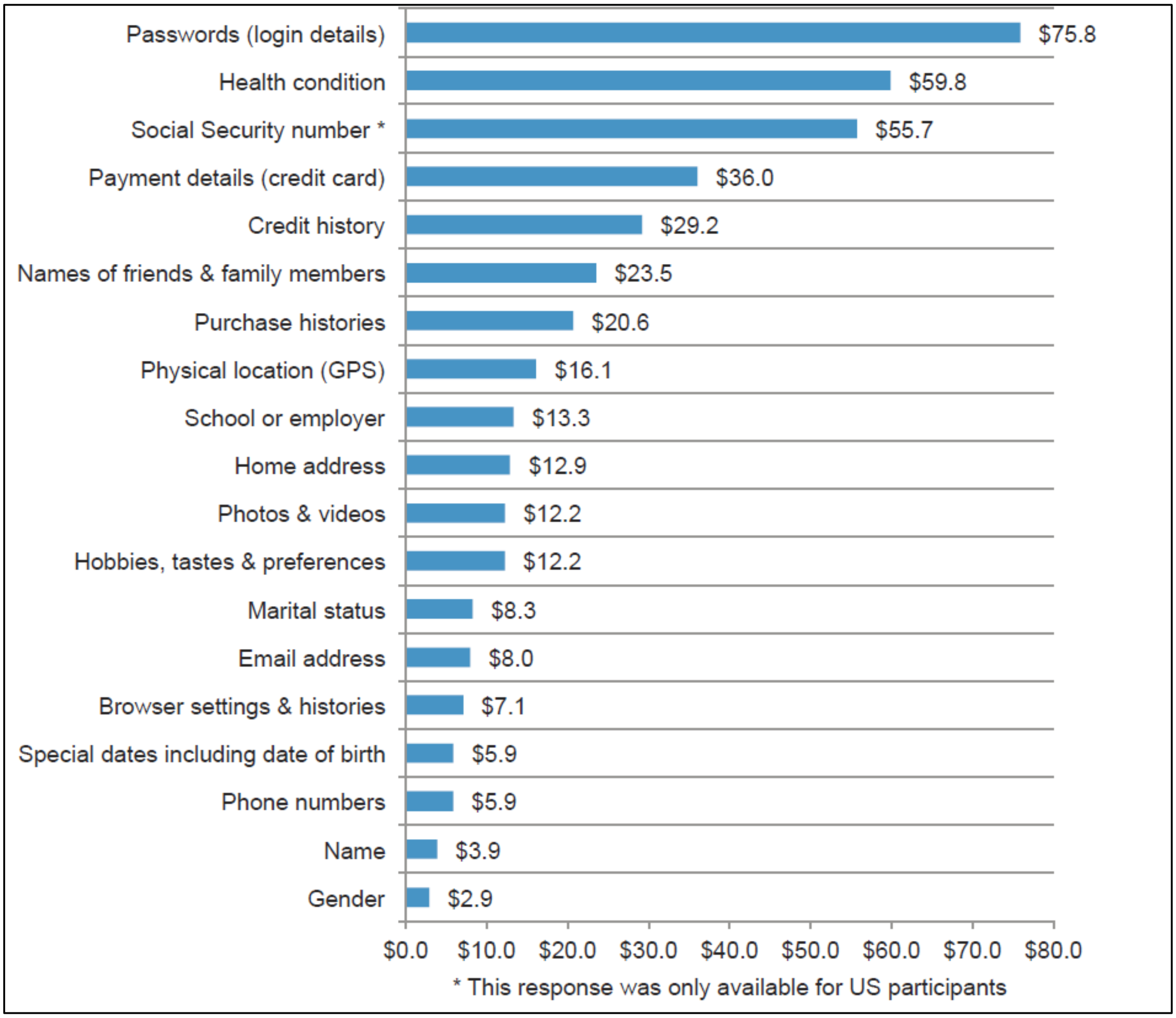
265. The first paragraph of the Website Privacy Statement distinguishes between how Rush treats "users" of the website versus "patients" who are protected by the Rush "patient care privacy policy," which is link the Notice of Privacy Practices, thereby incorporating the Notice of Privacy Practices into the Website Privacy Statement for patients.

266. The rest of the Website Privacy Statement is consistent with the data license that Rush states in the Notice of Privacy Practices and MyChart patient portal Terms and Conditions. Specifically, Rush states that the data license price does not include any personal information or the sharing of any information with third parties: (1) "We do not collect any personally identifiable information unless users voluntarily supply it as part of a request for service or information;" (2) "We do not share information collected through the website with any third-party advertisers;" and (3) "For information on security of communications between Rush … and patients, please see the patient privacy information on this site."

267. By collecting, using, and sharing patient information with Facebook, Google, and others for marketing purposes in excess of the data license price that Rush stated in its Notice of Privacy Practices, MyChart patient portal Terms and Conditions, and Website Privacy Policy, Rush overcharged patients by granting itself a data license in excess of the price that it promised to patients.

268. The "data license" overcharge that Rush collects, uses, and shares for marketing purposes without authorization has monetary value.

269. For example, a 2015 study found respondents placed a value of $59.80 on health information.



270. In addition, some companies sell de-identified health information in the open market. For example, a company named Prognos Health provides a data platform where it purports to sell information from “more than 325 million de-identified patients.”

271. Because Americans typically do not want to sell their personal health information for any purpose and it is illegal to even share such information without express, written

authorization, there are fewer open markets for a license to collect or sell personal health information for non-health purposes than other types of data. However, black markets do exist for such data. It has been reported that health data can be "more expensive than stolen credit card numbers" on black markets.

CLASS ACTION ALLEGATIONS

272. Plaintiff re-alleges and incorporates by reference the allegations set forth above.

273. Plaintiffs bring this action as a class action pursuant to Rules 23(a), 23(b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of a Class, defined as follows:

> **Patient Class**
> During the fullest period allowed by law, all persons who are, or were, patients of Rush or any of its affiliates and accessed Rush's MyChart patient portal that causes transmission of personally identifiable data and communications to be made to third-parties.

274. Excluded from the Class are Rush and any of its members, affiliates, parents, subsidiaries, officers, directors, employees, successors, or assigns; and the Court staff assigned to this case and their immediate family members. Plaintiffs reserve the right to modify or amend the Class definition, as appropriate, during the course of this litigation.

275. This action has been brought and may properly be maintained on behalf of the Class proposed herein under the criteria of Rule 23 of the Federal Rules of Civil Procedure.

276. **Numerosity—Federal Rule of Civil Procedure 23(a)(1)** – Class members are so numerous that their individual joinder is impracticable. The precise number of Class members and their identities are unknown to Plaintiffs at this time but will be determined through discovery through the records of the Defendant.

277. **Commonality and Predominance—Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3)** – Common questions of law and fact exist and predominate over questions affecting only individual Class members. These common legal and factual questions include the following:

a. Whether Defendant's practices relating to disclosures of Plaintiffs' and patient Class members' personally identifiable data and communications to third parties were intentional;

b. Whether Defendant profited from disclosures to the third parties;

c. Whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq*.;

d. Whether Defendant's practices alleged herein were unfair, deceptive, and/or unlawful in any respect, thereby violating the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq*.;

e. Whether Defendant's practices alleged herein were unfair trade practices, thereby violating the Illinois Deceptive Trade Practices Act, 815 ILCS 510/1 *et seq*.;

f. Whether Defendant's practices constitute an unauthorized intrusion upon seclusion;

g. Whether Defendant's practices constitute breach of implied duty of confidentiality;

h. Whether Defendant's conduct harmed and continues to harm Plaintiffs and Class members, and if so, the extent of the injury;

i. Whether and to what extent Plaintiffs and Class members are entitled to damages and other monetary relief;

j. Whether and to what extent Plaintiffs and Class members are entitled to equitable relief, including, but not limited to, a preliminary and/or permanent injunction; and

k. Whether and to what extent Plaintiffs and Class members are entitled to attorney fees and costs.

278. **Typicality—Federal Rule of Civil Procedure 23(a)(3)** – Plaintiffs' claims are typical of the claims of the Class and Plaintiffs have substantially the same interest in this matter

as other Class members. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of the other members of the Class. Plaintiffs' claims arise out of the same set of facts and conduct as all other Class members. Plaintiffs and all Class members are patients of Rush who used the Defendant's web-property set-up by Rush for patients, and are victims of Rush's unauthorized disclosures to third-parties. All claims of the Plaintiffs and Class members are based on Rush's wrongful conduct and unauthorized disclosures.

279. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4)** – Plaintiffs will fairly and adequately protect the interests of Class members. Plaintiffs have retained competent counsel experienced in complex class action privacy litigation and Plaintiffs will prosecute this action vigorously. Plaintiffs have no interests adverse or antagonistic to those of the Class.

280. **Declaratory and Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2)** – Rush acted or refused to act on grounds generally applicable to Plaintiffs and the other Class members, thereby making appropriate final injunctive relief and/or declaratory relief, as described below.

281. **Superiority—Federal Rule of Civil Procedure 23(b)(3)** – A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are small compared with the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done them. Furthermore, even if Class members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts.

Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

282. Additionally, the Class may be certified under Rule 23(b)(1) or (b)(2) because:

a. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Defendant;

b. The prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and/or

c. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final and injunctive relief with respect to the Class members as a whole.

COUNT I.
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2510 *et seq.*
On Behalf of Plaintiffs and the Class

283. Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

284. The ECPA protects both the sending and receipt of communications.

285. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral, or electronic communication is intercepted.

286. A violation of the ECPA occurs where any person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any . . . electronic communication" or "intentionally discloses, or endeavors to disclose, to any other person the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication" or "intentionally uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication." 18 U.S.C. §§ 2511(1)(a), (c)-(d).

287. "Intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

288. "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

289. "Contents" includes "any information relating to the substance, purport, or meaning" of the communication at issue. 18 U.S.C. § 2510(8).

290. An "electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

291. Plaintiffs and Patient Class members' interactions with Rush's web properties, including the MyChart patient portal, and their online communications with Rush are electronic communications under the ECPA.

292. Whenever Plaintiffs and Patient Class members interacted with Rush's web properties, including Rush's MyChart patient portal, Rush, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally intercepted, and endeavored to intercept Plaintiffs' and Patient Class members' electronic communications without authorization or consent.

293. Whenever Plaintiffs and Patient Class members interacted with Rush's web properties, including Rush's MyChart patient portal, Rush, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiffs' and Patient Class members' electronic communications to third parties, including Facebook, Google, and Bidtellect, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA.

294. Whenever Plaintiffs and Patient Class members interacted with Rush's web properties, including Rush's MyChart patient portal, Rush, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiffs' and Patient Class members' electronic communications, for purposes other than providing health care services to Plaintiffs and Patient Class members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA.

295. Whenever Plaintiffs and Patient Class members interacted with Rush's web properties, including Rush's MyChart patient portal, Rush, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally redirected the contents of Plaintiffs' and Class members' electronic communications while those communications were in

transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook, Google, and Bidtellect.

296. Whenever Plaintiffs and Patient Class members interacted with Rush's web properties, including Rush's MyChart patient portal, Rush, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally divulged the contents of Plaintiffs' and Class members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook, Google, and Bidtellect.

297. Rush intentionally intercepted and used the contents of Plaintiffs' and Patient Class members' electronic communications for the unauthorized purpose of disclosing and, on information and belief, profiting from, Plaintiffs' and Patient Class members' communications by selling the contents to third parties including Facebook, Google, and Bidtellect.

298. Plaintiffs and Patient Class members did not authorize Rush to acquire the content of their communications for purposes of sharing and selling the personal information contained therein.

299. The ECPA provides that a "party to the communication" may liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."

300. Rush is a "party to the communication" with respect to patient communications.

301. Rush's acquisition of patient communications that were used and disclosed to Facebook, Google, and others was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and of Illinois, including:

a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;

b. Violation of the Illinois Computer Fraud Act, 720 ILCS 5/17-50;

c. Violation of the Illinois Computer Crime Prevention Law, 720 ILCS 5/17-51; and

d. Violation of the Illinois Deceptive Trade Practices Act, 815 ILCS §§ 510/2, *et seq*.

302. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to "use[] or cause[] to be used a unique health identifier" or to "disclose[] individually identifiable health information to another person … without authorization" from the patient.

303. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

304. Rush's conduct violated 42 U.S.C. § 1320d-6 in that it:

a. Used and caused to be used fbp, ga, and gid cookies associated with specific patients without patient authorization;

b. Disclosed individually identifiable health information to Facebook, Google, and others.

305. Rush's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Rush's use of the Facebook and Google source code was for Rush's commercial advantage to increase revenue from existing patients and gain new patients.

306. Under 720 ILCS, 17-50, "[a] person commits computer fraud when he or she knowingly:

a. Accesses or causes to be accessed a computer or any part therefor, or a program or data, with the intent of device or executing any scheme or artifice to defraud, or as part of a deception;

b. Obtains use of, damages, or destroys a computer or any part thereof, or alters, deletes, or removes any program or data contained therein, in connection with any scheme or artifice to defraud, or as part of a deception; or

c. Access or causes to be accessed a computer or any part thereof, or a program or data, and obtains money or control over any such money, property, or services of another in connection with any scheme or artifice to defraud, or as part of a deception.

307. Rush's conduct violated the Illinois Computer Fraud Act in that:

a. Rush accessed Plaintiffs' and Class members' computing devices and data as part of a deception and without their authorization, including through placement of the fbp, ga, and gid cookies as well as use of source code that commanded Plaintiffs' and Class members' computing devices to send identifiers and the content of communications with Rush simultaneously to Rush and Facebook, Google, and others;

b. Rush obtained use of or and removed data from Plaintiffs' and Class members' computing devices as part of a deception and without their authorization, including through placement, use, and removal of the fbp, ga, and gid cookies as well as use of source code that commanded Plaintiffs' and Class members' computing devices to send identifiers and the content of communications with Rush simultaneously to Rush and Facebook, Google, and others;

c. Rush accessed or caused to be accessed the Plaintiffs' and Class members' computing devices and data, and thereby obtained control over the Plaintiffs' and Class members' property in the form of their computing devices and right to control access and use of their personal health information as part of a deception and without their authorization, including through placement of the fbp, ga, and gid cookies as well as the use of source code that commanded Plaintiffs' and Class members' computing devices to send identifiers and the content of communication with Rush simultaneously to Facebook, Google, and others.

308. The Illinois Computer Crime Prevention Law ("ICCPL") prohibits "computer tampering," and provides a private right of action for whoever "suffers loss by reason of a violation of subdivision (a)(4)." 720 ILCS 5/17-51(c).

309. Subdivision (a)(4) of the ICCPL provides:

> (a) A person commits computer tampering when he or she knowingly and without the authorization of a computer's owner or in excess of the authority granted to him or her: … (4) Inserts or attempts to insert a program into a computer or computer program knowing or having reason to know that such program contains information or commands that will or may…(b) alter, delete, or remove a computer program or data from that computer, or any other computer program or data in a computer subsequently accessing or being accessed by that computer; or (c) cause loss to the users of that computer or the users of a computer which accesses or which is accessed by such program…

310. Rush violated the ICCPL when it knowingly and without Plaintiffs' or Class members' authorization inserted the fbp, ga, and gid cookies on Plaintiffs' and Class members' computing devices.

311. The fbp, ga, and gid cookies, which constitute programs, commanded Plaintiffs' and Class members' computing devices to remove and redirect their data and the content of their communications with Rush to Google, Facebook, and others.

312. Rush knew or had reason to know that the fbp, ga, and gid cookies would command Plaintiffs' and Class members' computing devices to remove and redirect their data and the content of their communications with Rush to Google, Facebook, and others.

313. Rush knew or had reason to know that its use of the fbp, ga, and gid cookies would cause Plaintiffs and Class members to suffer a loss, including:

a. The interruption or preclusion of Plaintiffs' and Class members' ability to communicate with their health care providers on their health care providers' or websites;

b. The diminution in value of Plaintiffs' and Class members' protected health information;

c. Plaintiffs' and Class members' inability to use their computing devices for the purpose of communicating with their health care providers;

d. The loss of privacy due to Rush making sensitive and confidential information such as patient status, test results, and appointments that Plaintiffs and Class members intended to remain private no longer private; and

e. Rush took something of value from Plaintiffs and Class members and derived benefits therefrom without Plaintiffs' and Class members' knowledge or informed consent and without sharing the benefit of such value.

314. Rush's acquisition of patient communications that Rush used and disclosed to Facebook, Google, and others was done in violation of the Illinois Deceptive Trade Practices Act, as alleged below in Count III.

315. Rush's acquisition of patient communications that Rush used and disclosed to Facebook, Google, and others was done for purposes of committing trespass to chattels, as alleged below, in that it was accomplished through source code that cause Facebook and Google cookies (including but not limited to the fbp, ga, and gid cookies) to be deposited on Plaintiffs' and Class members' computing devices as "first-party" cookies that are not blocked.

316. As a direct and proximate result of Rush's violation of the ECPA, Plaintiffs and Class members were damaged by Rush's conduct in that:

a. Rush harmed Plaintiffs' and Class members' interest in privacy;

b. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no more;

c. Rush eroded the essential confidential nature of the provider-patient relationship;

d. Rush took something of value from Plaintiffs and Class members and derived benefit therefrom without Plaintiffs' and Class members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Class members did not get the full value of the medical services for which they paid, which included Rush's duty to maintain confidentiality; and

f. Rush's actions diminished the value of Plaintiffs and Class members' personal information.

317. Plaintiffs, individually, on behalf of the Class members, seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages, punitive damages, preliminary and other equitable or declaratory relief, and attorneys' fees and costs.

COUNT II.
BREACH OF THE IMPLIED DUTY OF CONFIDENTIALITY
<u>On Behalf of Plaintiffs and the Class</u>

318. Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

319. Plaintiffs and Class members were patients of Rush and received health care services from Rush.

320. As part of establishing and continuing the health care services provider/patient relationship between Rush and its patients, including Plaintiffs and Class members, Rush agreed to keep Plaintiffs' and Class members information confidential.

321. There is a duty of confidentiality implied in every health care provider and patient relationship, akin to an implied contract, such that health care services providers may not disclose confidential information acquired through the health care provider-patient relationship. *See, e.g.*, *Geisberger v. Willuhn*, 72 Ill. App. 3d 435, 438 (1979).

322. The implied duty of confidentiality is at least as extensive as Rush's statutory obligations as a health care services provider to maintain patient confidentiality.

323. Under the Illinois' Medical Patient Rights Act ("MPRA") "health care provider[s]" must "refrain from disclosing the nature or details of services provided to patients." 410 ILCS § 50/3.

324. Under 735 ILCS 5/8-802, "[n]o physician or surgeon shall be permitted to disclose any information he or she may have acquired in attending any patient in a professional character."

325. The information Rush patients provide to Rush via Rush's MyChart patient portal is information acquired in attending a patient.

326. Rush is obligated to protect the confidentiality of patient information under HIPPA.

327. Rush also may not disclose personally identifiable information about a patient, potential patient, or household member of a patient for marketing purposes without the patient's express written authorization. *See* HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501; 164.508(a)(3), 164.514(b)(2)(i).

328. HIPAA preempts any state law that is less protective of patient privacy.

329. To the extent the Court determines that Illinois state law is less protective of patient privacy than HIPAA, then that Illinois law is pre-empted by HIPAA.

330. Rush's web property, www.rush.edu, links to a HIPAA notice that acknowledges Rush's duty of confidentiality, including assuring Plaintiffs and Class members that Rush will protect the confidentiality of their data and communications. The notice further assures Plaintiffs and Class members that Rush will not use their data and communications for marketing purposes without express written authorization.

331. Rush provided its HIPAA notice to Plaintiffs and all Rush patients.

332. The HIPAA Notice is incorporated by reference into the Terms and Conditions that Rush makes a condition of signing-up for and using Rush's MyChart patient portal.

333. The Terms and Conditions for Rush's MyChart patient portal can be found at: https://mychart.rush.edu/MyChart/Authentication/Login?mode=stdfile&option=termsandconditions.

334. Rush did not adequately provide notice of any website privacy policies to Plaintiffs or patients.

335. Plaintiffs and Class members performed all required conditions of their implied contracts with Rush.

336. Rush breached the implied duty of confidentiality to Plaintiffs and Class members by intentionally deploying source code at its web properties that caused the transmission of personally identifiable patient data and communications to third parties including Facebook, Google, and Bidtellect.

337. As a direct and proximate result of Rush's breach of the implied duty of confidentiality, Plaintiffs and Class members were damaged in that:

a. Rush harmed Plaintiffs' and Class members' interest in privacy;

b. Sensitive and confidential information that Plaintiffs and Class members intended to remain private is no more;

c. Rush eroded the essential confidential nature of the provider-patient relationship;

d. Rush took something of value from Plaintiffs and Class members and derived benefit therefrom without Plaintiffs' and Class members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Class members did not get the full value of the medical services for which they paid, which included Rush's duty to maintain the confidentiality of their patient information; and

f. Rush's actions diminished the value of Plaintiffs' and Class members' personal information.

COUNT III.
VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 ILCS §§ 510/2, *et seq*.
<u>On Behalf of Plaintiffs and the Class</u>

338. Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

339. Rush is a "person" as defined by 815 ILCS § 510/1(5).

340. Rush engaged in deceptive trade practices in the conduct of its business, in violation of 815 ILCS § 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

341. Rush's practice of disclosing Plaintiffs' and Class members' personally identifiable data and re-directing their communications to third parties without authorization, consent, or knowledge is a deceptive trade practice, in violation of 815 ILCS § 510/2(a).

342. Rush's practice of disclosing Plaintiffs' and Class members' personally identifiable data and re-directing their communications to third parties without authorization, consent, or knowledge was willful.

343. Rush's practice of disclosing Plaintiffs' and Class members' personally identifiable data and re-directing their communications to third parties without authorization, consent, or knowledge was intentional.

344. Rush's representations and omissions were material because they were likely to deceive reasonable consumers about the privacy, security, and use of their personally identifiable patient data and communications when using the Rush web property, including the MyChart patient portal.

345. The above unfair and deceptive practices and acts by Rush were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and the Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

346. As a direct and proximate result of Rush's unfair, unlawful, and deceptive trade practices, Plaintiffs and the Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including overpaying for Rush's health care services; and loss of value of their personally identifiable patient data and communications.

347. As a direct and proximate result of Rush's unfair, unlawful, and deceptive acts and practices, Plaintiffs and the Class members were also damaged by Rush's conduct in that:

a. Rush harmed Plaintiffs' and Class members' interest in privacy;

b. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no more;

c. Rush eroded the essential confidential nature of the provider-patient relationship;

d. Rush took something of value from Plaintiffs and Class members and derived benefit therefrom without Plaintiffs' and Class members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Class members did not get the full value of the medical services for which they paid, which included Rush's duty to maintain confidentiality; and

f. Rush's actions diminished the value of Plaintiffs and Class members' personal information.

348. Plaintiffs and the Class members are patients of Rush and need access to Rush's web properties, including www.rush.edu and the MyChart portal, in connection with receiving health care from Rush. Because Plaintiffs and Class members need to, and so will continue to use Rush's web properties in the future, if Rush's unfair, unlawful, and deceptive trade practices are allowed to continue, Plaintiffs and Class members are likely to suffer continuing harm in the future.

349. Plaintiffs and the Class members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

COUNT IV.
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
815 ILCS §§ 505/1, *et seq.*
<u>On Behalf of Plaintiffs and the Class</u>

350. Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

351. Rush is a "person" as defined by ILCS § 505/1(c).

352. Plaintiffs and the other Class members are "consumers" as defined by 815 ILCS § 505/1(e).

353. Rush's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 ILCS. § 505/1(f).

354. Rush's unfair acts and practices against Plaintiffs and the other Class members occurred in the course of trade or commerce in Illinois, arose out of transactions that occurred in Illinois, and/or harmed individuals in Illinois.

355. Plaintiffs and Class members received and paid for health care services from Rush.

356. Plaintiffs and Class members used Rush's web properties, including the MyChart patient portal, in connection with receiving health care services from Rush.

357. Plaintiffs' and Class members' payments to Rush for health care services were for household and personal purposes.

358. Rush's practice of disclosing Plaintiffs' and Class members' personally identifiable data and re-directing their communications to third parties without authorization, consent, or

knowledge is a deceptive, unfair, and unlawful trade act or practice, in violation of 815 ILCS § 505/2.

359. Rush's unfair business practices were targeted at all Rush patients, including Plaintiffs and the other Class members.

360. Rush's representations and omissions were material because they were likely to deceive reasonable consumers about the privacy, security, and use of their personally identifiable patient data and communications when using the Rush web property, including the MyChart patient portal.

361. Rush intended to mislead Plaintiffs and the other Class members and induce them to rely on its misrepresentations and omissions.

362. Rush's surreptitious collection and disclosure of Plaintiffs' and Class members' personally identifiable data and communications to third parties involves important consumer protection concerns.

363. Plaintiffs and the Class members were injured and have suffered damages as a direct and proximate result of Rush's unfair acts and practices.

364. Plaintiffs' and the Class members' injuries were proximately caused by Rush's unfair and deceptive business practices.

365. As a result of Rush's conduct, Rush has been unjustly enriched.

366. The above unfair and deceptive practices and acts by Rush were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and the Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

367. As a direct and proximate result of Rush's unfair, unlawful, and deceptive trade practices, Plaintiffs and the Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including overpaying for Rush's health care services, and loss of value of their personally identifiable patient data and communications.

368. As a direct and proximate result of Rush's unfair, unlawful, and deceptive acts and practices, Plaintiffs and the Class members were also damaged by Rush's conduct in that:

a. Rush harmed Plaintiffs' and Class members' interest in privacy;

b. Sensitive and confidential information that Plaintiff and the Class members intended to remain private is no more;

c. Rush eroded the essential confidential nature of the provider-patient relationship;

d. Rush took something of value from Plaintiffs and the Class members and derived benefit therefrom without Plaintiffs' and the Class members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and the Class members did not get the full value of the medical services for which they paid, which included Rush's duty to maintain confidentiality; and

f. Rush's actions diminished the value of Plaintiffs and the Class members' personal information.

369. The relief requested by Plaintiffs and the other Class members, would provide redress for the harms Rush caused not just to Plaintiffs, but to all other Class members.

370. Plaintiffs and the Class members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

COUNT V.
INVASION OF PRIVACY – INTRUSION UPON SECLUSION
<u>On Behalf of Plaintiffs and the Class</u>

371. Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

372. Plaintiffs' and Class members' communications with Rush constitute private conversations, matters, and data.

373. Plaintiffs and Patient Class members have a reasonable expectation that Rush would not disclose personally identifiable patient data and communications to third parties for marketing purposes without Plaintiffs and other Class members authorization, consent, knowledge, or any further action on the patient's part.

374. In addition, Plaintiffs and Class members have a reasonable expectation that Rush will not place tracking devices on its own patients' communications devices without their knowledge or consent.

375. Rush intruded upon Plaintiffs and Class members seclusion by deploying source code on its web properties that caused cookies associated with Facebook and Google to be deposited on Plaintiffs' and Class members communications devices as first-party cookies used for tracking purposes.

376. Rush did not have Plaintiffs' or any Class members' consent to deposit tracking tools associated with Facebook or Google onto the Plaintiffs' or Class members' computing devices.

377. Rush designed its web properties so that it would be impossible for Plaintiffs and Class members to avoid Rush depositing Facebook and Google first-party cookies on their

communications devices if Plaintiff or other Patient Class members sought to use the Rush patient portal.

378. Rush's actions in depositing Google and Facebook cookies on the Plaintiffs' and Class members' communications devices would be highly offensive to a reasonable person.

379. In June 2022, a publication called The Markup reported that "Facebook is Receiving Sensitive Medical Information from Hospital Websites."

380. The article quoted numerous experts, none of which defended the practice of hospitals incorporating such tools onto their properties.

381. David Holtzman, described as a "health privacy consultant who previously served as a senior privacy advisor in the U.S. Department of Health and Human Services' Office of Civil Rights and whose LinkedIn profile states that he served as a consultant for "healthcare organizations in defense of claims or regulatory actions alleging inadequate information privacy and security standards," stated:

a. "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it. I cannot say [sharing this data] is for certain a HIPAA violation. It is quite likely a HIPAA violation."

b. "When an individual has sought out a provider and indicated that they want to make an appointment, at that point, any individually identifiable health information that they've provided in this session, in the past, or certainly in the future, is protected under HIPAA and could not be shared with a third party like Facebook."

382. Iliana Peters, described as "a privacy lawyer with the firm Polsinelli who previously headed HIPAA enforcement for the Office for Civil Rights, stated, "Generally, HIPAA covered

entities and business associates should not be sharing identifiable information with social media companies unless they have HIPAA authorization [from the individual] and consent under state law."

383. Glenn Cohen, described as the "faculty director of Harvard Law School's Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics, stated, "Almost any patient would be shocked to find out that Facebook is being provide an easy way to associate their prescriptions with their name. Even if perhaps there's something in the legal architecture that permits this to be lawful, it's totally outside the expectations of what patients think the health privacy laws are doing for them."

384. State and federal judges have expressed similar sentiments:

a. Several state courts have found that similar allegations stated privacy claims that require conduct that would be considered "highly offensive" to a reasonable person. *See Doe v. Virginia Mason*, 2020 WL 1983046, at *2 (Wash. Super. Feb. 12, 2020); *Doe v. Medstar*, Case No. 24-C-20-000591 (Baltimore City, Maryland); *Doe v. University Hospitals*, Case No. CV-20-9333357 (Cuyahoga County, Ohio) (privacy torts merged for medical privacy); *Doe v. Mercy Health*, Case No. A 2002633 (Hamilton County, Ohio) (same)); (*Doe v. Partners*, Case No. 1984-CV-01651 (Suffolk County, Massachusetts)).

b. In *In re Meta Pixel Healthcare Litigation*, N.D. Cal. Case No. 22-cv-3580, the Honorable Judge William Orrick stated that users would be "shocked to realize" the data collection that occurs as a result of hospitals' use of

Facebook tracking tools. *In re Meta Pixel Healthcare Litigation* Nov. 9, 2023 Hr'g Tr. at 20:15-16.

385. A health care provider may not place tracking devices on their patients' property without the patient's knowledge and authorization.

386. Plaintiffs and Class members did not authorize, consent, know about, or take any action to indicate consent to Rush's conduct alleged herein.

387. Plaintiffs' and Class members' personally identifiable data and communications are the type of sensitive, personal information that one normally expects will be protected from disclosure to unauthorized parties by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs' and Class members' personally identifiable data and communications, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

388. Rush's conduct described herein was intentional.

389. Rush's willful and reckless conduct in allowing access to and disclosure of Plaintiffs' and Class members' sensitive, personally identifiable data and communications to unauthorized third parties is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

390. As a direct and proximate result of Rush's intrusion upon their seclusion, Plaintiffs and Class members were damaged by Rush's intrusion in that:

a. Rush harmed Plaintiffs' and Class members' interest in privacy;

b. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no more;

c. Rush eroded the essential confidential nature of the provider-patient relationship;

d. Rush took something of value from Plaintiffs and Class members and derived benefit therefrom without Plaintiffs' and Class members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Class members did not get the full value of the medical services for which they paid, which included Rush's duty to maintain confidentiality; and

f. Rush's actions diminished the value of Plaintiffs and Class members' personal information.

391. As a result of the invasion of privacy caused by Rush, Plaintiffs and Class members suffered and will continue to suffer damages and injury as set forth herein.

392. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

COUNT VI.
INVASION OF PRIVACY – PUBLICATION OF PRIVATE FACTS
On Behalf of Plaintiffs and the Class

393. Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

394. Plaintiffs' and Class members' communications with Rush constitute private conversations, matters, facts, and data.

395. Plaintiffs and Class members have a reasonable expectation that Rush would not disclose personally identifiable patient data and communications to third parties for marketing purposes without Plaintiffs and other Class members authorization, consent, knowledge, or any further action on the patient's part.

396. In addition, Plaintiffs and Class members have a reasonable expectation that Rush will not place tracking devices on its own patients' communications devices without their knowledge or consent.

397. Rush, a health care provider, has a duty to keep personally identifiable patient data and communications confidential.

398. Rush expressly promised to maintain the confidentiality of personally identifiable patient data and communications in its HIPAA Notice of Privacy Practices and Web and Internet Policies.

399. Rush unlawfully published Plaintiffs' and Class members' private facts by deploying source code that caused the transmission of Plaintiffs' and Class members' personally identifiable data and the contents of communications Plaintiffs and Class members exchanged with their health care providers to third parties including Facebook, Google, and Bidtellect.

400. Plaintiffs and Class members did not authorize, consent to, know about, or take any action to indicate consent to Rush's conduct alleged herein.

401. Plaintiffs' and Class members' personally identifiable data and communications are the type of sensitive, personal information that one normally expects will be protected from disclosure to unauthorized parties by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs' and Class members' personally identifiable data and communications, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

402. Rush's conduct described herein was intentional.

403. Rush's conduct in disclosing Plaintiffs' and Class members' personally identifiable data and communications to third parties was and is highly offensive to a reasonable person.

404. Rush's willful and reckless conduct in disclosing Plaintiffs' and Class members' sensitive, personally identifiable data and communications to unauthorized third parties is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

405. As a direct and proximate result of Rush's unlawful publication of their private facts, Plaintiffs and Class members were damaged by Rush's conduct in that:

a. Rush harmed Plaintiffs' and Class members' interest in privacy;

b. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no more;

c. Rush eroded the essential confidential nature of the provider-patient relationship;

d. Rush took something of value from Plaintiffs and Class members and derived benefit therefrom without Plaintiffs' and Class members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Class members did not get the full value of the medical services for which they paid, which included Rush's duty to maintain confidentiality; and

f. Rush's actions diminished the value of Plaintiffs and Class members' personal information.

406. As a result of the invasion of privacy caused by Rush, Plaintiffs and Class members suffered and will continue to suffer damages and injury as set forth herein.

407. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

COUNT VII.
TRESPASS TO CHATTELS
On Behalf of Plaintiffs and the Class

408. Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

409. Plaintiffs and Class members owned, leased, or controlled their computing devices from which they communicated with Rush.

410. As set forth below, Rush intentionally used, intermeddled, interfered with, and dispossessed Plaintiffs' and Class members' of their computing devices without their consent by placing the fbp, ga, and gid cookies on Plaintiffs' and Class members' computing devices, which caused Plaintiffs and Class members to suffer damages.

411. For security purposes, Plaintiffs and other patient Class members must enable first-party cookies to use the Rush patient portal.

412. Rush abuses this security purpose of first-party cookies for its patient portal by deploying source code that facilitates tracking through first-party cookies, which are *required* by Rush for any patient to use its patient portal.

413. The source deployed by Rush on its web properties is designed such that, when Plaintiffs and other Class members visit the Rush web properties, cookies associated with Facebook and Google are deposited on their communications devices.

414. For Facebook, the source code that Rush has deployed on its web properties deposits a cookie named "_fbp" on the patients' device.

415. For Google, the source code that Rush has deployed on its web properties deposits cookies named "_ga" and "_gid" on the patients' device.

416. Although they are cookies associated with the third-parties Facebook and Google, respectively, the fbp, ga, and gid cookies are deposited on the patients' communications device as "first-party" cookies associated with Rush.

417. By depositing the fbp, ga, and gid cookies as first-party cookies, Rush ensures that it is able to share each Plaintiff and Class members' identification numbers with Facebook and Google even if a patient attempted to block third-party cookies.

418. The Facebook "fbp" cookies are used to track Plaintiff and patient communications at www.rush.edu and to log-in to the Rush patient portal.

419. The Google "ga" and "gid" cookies are used to track Plaintiff and patient communications at www.rush.edu, to log-in to the Rush patient portal, and while patients are logged-in and communicating inside the patient portal.

420. Plaintiffs and Class members did not consent to Rush using source code that places cookies associated with Facebook and Google on their devices as "first-party" cookies.

421. Rush's placement of the Facebook and Google cookies as first-party cookies is the modern equivalent of placing a bug in someone's telephone or on the desk where their computer sits. The Facebook and Google source code and cookies deployed by Rush have taken the place of the "bug," which is why these tools are often called "web bugs."

422. Plaintiffs and Class members computing devices derive substantial value from their ability to facilitate communications with their health care providers or covered entities, which is integral to the intended function of their devices.

423. Rush's setting of Facebook and Google cookies results in the persistent and unavoidable interception of Plaintiffs' and Class members' communications, which deprives

Plaintiffs and Class members of the full value of using their computing devices for those communications.

424. Plaintiffs' and Class members' devices are useless for exchanging private communications with Rush, which substantially impairs the condition, quality, and value of Plaintiffs' and Class members' computing devices.

425. Rush's trespass onto Plaintiffs' and Class members' computing devices caused them the following damages:

a. Nominal damages for trespass;

b. The total deprivation of their use of their computing devices to privately communicate with Rush.

426. For Rush's trespass, Plaintiffs and Class members seek nominal damages, actual damages, general damages, unjust enrichment, punitive damages, and any other relief the Court deems just.

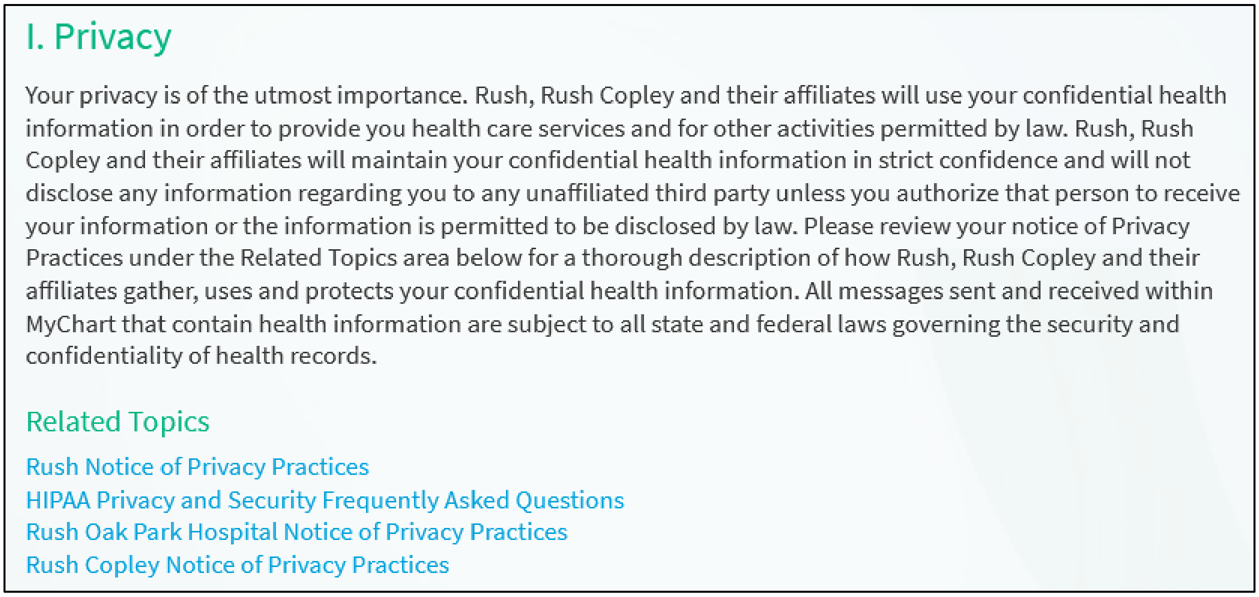
COUNT VIII.
BREACH OF CONTRACT
On Behalf of Plaintiffs and the Class

427. Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

428. Rush requires patients who use the MyChart patient portal to agree to "Terms and Conditions" to obtain access to the MyChart patient portal.

429. The "Terms and Conditions" is a binding contract on Rush.

430. The first paragraph of the patient portal terms and conditions promises:



I. Privacy

Your privacy is of the utmost importance. Rush, Rush Copley and their affiliates will use your confidential health information in order to provide you health care services and for other activities permitted by law. Rush, Rush Copley and their affiliates will maintain your confidential health information in strict confidence and will not disclose any information regarding you to any unaffiliated third party unless you authorize that person to receive your information or the information is permitted to be disclosed by law. Please review your notice of Privacy Practices under the Related Topics area below for a thorough description of how Rush, Rush Copley and their affiliates gather, uses and protects your confidential health information. All messages sent and received within MyChart that contain health information are subject to all state and federal laws governing the security and confidentiality of health records.

Related Topics

Rush Notice of Privacy Practices
HIPAA Privacy and Security Frequently Asked Questions
Rush Oak Park Hospital Notice of Privacy Practices
Rush Copley Notice of Privacy Practices

431. Rush breaches these contractual promises in numerous ways.

432. Rush has failed to "maintain [patient] confidential health information in strict confidence … unless you authorize that person to receive your information or the information is permitted to be disclosed by law" with respect to the patient portal because it:

a. routinely shared patient portal login information with Facebook; and

b. continues to share login, logout, and information about patient communications inside the portal with Google.

433. Rush has failed to "not disclose any information regarding you to any unaffiliated third party unless you authorize that person to receive your information or the information is permitted to be disclosed by law" with respect to the patient portal because it:

a. routinely shared patient portal login information with Facebook; and

b. continues to share login, logout, and information about patient communications inside the patient portal with Google.

434. The Rush MyChart patient portal contract promises that "Use of MyChart by Rush, Rush Copley, and their affiliates occurs over a secure connection." However, Rush breaches this

promise by re-directing patient identifiers and communications content to Google on login, logout, and inside the patient portal.

435. The Rush MyChart patient portal contract promises that "Rush, Rush Copley, and their affiliates afford the same degree of confidentiality to health information stored in MyChart as is given to health information stored by Rush, Rush Copley and their affiliates in any other medium." However, upon information and belief, Rush breaches this promise because it does not provide patient identifiers or communications content to Google anywhere outside the patient portal.

436. The Rush MyChart patient portal contract promises that, "Rush, Rush Copley and their affiliates has taken steps to make all information received from our online visitors as secure as possible against unauthorized access and use." However, Rush breaches this promise by re-directing patient identifiers and communications content to Google.

437. The Rush MyChart patient portal contract promises, that, when communicating with Rush, "If the URL beings with https:// (instead of http://), the document comes from a secure server. This means your data cannot be read or deciphered by unauthorized individuals." However, Rush breaches this promise by re-directing patient identifiers and communications content to Google.

438. As a direct and proximate result of Rush's breaches of contract, Plaintiffs and Class members did not receive the full benefit of the bargain of their contract with Rush in that Rush overcharged Plaintiffs and Class members by collecting data in excess of the "data license" that was agreed upon in the contract between Plaintiffs and Class members and Rush in the Rush Notice of Privacy Practices and the Rush MyChart patient portal Terms and Conditions. Specifically, as

set forth above, Rush expressly promised that its "data license" would not include the divulgence or sale of Plaintiffs' and Class members' confidential health information.

439. As a direct and proximate result of Rush's breaches of contract, Plaintiffs and the Class members suffered the following damages:

a. Nominal damages;

b. The interruption of preclusion of Plaintiffs' and Class members' ability to communicate with their health care providers on Rush's web properties;

c. The diminution in value of Plaintiffs' and Class members' protected health information;

d. Plaintiffs' and Class members' inability to use their computing devices for the purpose of communicating with their health care providers;

e. The loss of privacy due to Rush making sensitive and confidential information such as patient status and appointments that Plaintiffs and Class members intended to remain private no longer private;

f. Rush took something of value from Plaintiffs and Class members and derived benefits therefrom without Plaintiffs' and Class members' knowledge or informed consent and without sharing the benefit of such value; and

g. The deprivation of the benefit of the bargain in the Rush's contract stated that the data license for its services did not include the divulgence or sale of their confidential health information, but Rush took more data than the contractually agreed-upon amount.

440. For Rush's breaches of contract, Plaintiffs and Patient Class members seek nominal damages, general damages, compensatory damages, consequential damages, unjust enrichment, restitution, and any other relief the Court deems just.

COUNT IX.
BREACH OF THE DUTY OF GOOD FAITH AND FAIR DEALING
<u>On Behalf of Plaintiffs and the Class</u>

441. Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

442. A valid contract exists between Rush and each of the Plaintiffs and Patient Class members.

443. A duty of good faith and fair dealing is implied in every contract.

444. The duty of good faith and fair dealing obligates the parties to a contract to cooperate with each other so that each may obtain the full benefit of performance.

445. The duty of good faith and fair dealing also arises when the contract gives one party discretionary authority to determine a contract term.

446. Rush has discretionary authority to determine the meaning of the MyChart patient portal Terms of Use, including the terms governing Rush's maintenance of the privacy, confidentiality, and security of patients' confidential health information.

447. Rush abused its power to define terms of the contract between Rush and patients using the MyChart patient portal, including:

a. The meaning of the term "strict confidence" in Rush's promise that it "will maintain your confidential health information in strict confidence and will not disclose any information regarding you to any unaffiliated third party unless you authorize that person to receive your information or the information is permitted to be disclosed by law."

b. The meaning of the term "secure as possible" in Rush's promise that "Rush, Rush Copley and their affiliates has taken steps to make all information received from our online visitors as secure as possible against unauthorized access and use."

c. The meaning of the term "same degree of confidentiality" in Rush's promise that it "afford[s] the same degree of confidentiality to health information stored in MyChart as is given to health information stored by Rush, Rush Copley and their affiliates in any other medium."

d. The meaning of the term "use or disclose your medical information" in Rush's promise that it will not "use or disclose your medical information for marketing without your prior written authorization[.]"

e. The meaning of the term "sale of Protected Health Information" in Rush's promise that it "will request your authorization for certain marketing activities, including any activities that involve the sale of Protected Health Information."

448. Rush did not act fairly and good faith.

449. Rather than maintaining Plaintiffs' and Class members' confidential health information in "strict confidence," Rush disclosed Plaintiffs' and Class members' confidential health information to Facebook, Google, and other third parties.

450. Rather than taking "steps to make all information received from our online visitors as secure as possible," Rush designed its web properties to deploy third-party tracking technologies that caused Plaintiffs' and Class members' to be redirected and intercepted by third-party marketing companies.

451. Rather than affording "the same degree of confidentiality to health information stored in MyChart as is given to health information stored by Rush, Rush Copley and their affiliates in any other medium," Rush provided less confidentiality to patient identifiers or communications content obtained from and stored in the MyChart patient portal than those stored by Rush in any other medium.

452. Rather than refraining from using or disclosing Plaintiffs' and Patient Class members' health information for marketing without their consent, Rush did the exact opposite and divulged health information to Facebook, Google, and other advertisers.

453. Rather than requesting Plaintiffs' and Patient Class members' authorization for certain marketing activities, including activities that involve the sale of their Protected Health Information, Rush disclosed Plaintiffs' and Patient Class members' protected health information to third-party marketing companies without their knowledge, consent, or authorization.

454. In doing so, Rush frustrated and undercut Plaintiffs' and Patient Class members' contractual rights, and unfairly interfered with Plaintiffs' and Class members' rights under the parties' contract.

455. As a direct and proximate result of Rush's breaches, Plaintiffs and Class members did not receive the full benefit of the bargain of their contract with Rush in that Rush overcharged Plaintiffs and Class members by collecting data in excess of the "data license" that was agreed upon in the contract between Plaintiffs and Class members and Rush in the Rush Notice of Privacy Practices and the Rush MyChart patient portal Terms and Conditions. Specifically, as set forth above, Rush expressly promised that its "data license" would not include the divulgence or sale of Plaintiffs' and Class members' confidential health information.

456. As a direct and proximate result of Rush's breaches of the duty of good faith and fair dealing, Plaintiffs and the Class members suffered the following damages:

a. Nominal damages;

b. The interruption of preclusion of Plaintiffs' and Class members' ability to communicate with their health care providers on Rush's web properties;

c. The diminution in value of Plaintiffs' and Class members' protected health information;

d. Plaintiffs' and Class members' inability to use their computing devices for the purpose of communicating with their health care providers;

e. The loss of privacy due to Rush making sensitive and confidential information such as patient status and appointments that Plaintiffs and Class members intended to remain private no longer private;

f. Rush took something of value from Plaintiffs and Class members and derived benefits therefrom without Plaintiffs' and Class members' knowledge or informed consent and without sharing the benefit of such value; and

g. The deprivation of the benefit of the bargain in the Rush's contract stated that the data license for its services did not include the divulgence or sale of their confidential health information, but Rush took more data than the contractually agreed-upon amount.

457. For Rush's breaches of the duty of good faith and fair dealing, Plaintiffs and Class members seek nominal damages, general damages, compensatory damages, consequential damages, unjust enrichment, restitution, and any other relief the Court deems just.

COUNT X.
QUASI-CONTRACT
(Pleaded in the alternative to Counts XIII and IX)
<u>On Behalf of Plaintiffs and the Class</u>

458. Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

459. Rush has wrongfully and unlawfully transmitted Plaintiffs' and Patient Class members' individually identifiable health information without their consent.

460. Plaintiffs' and Class members' individually identifiable health information conferred an economic benefit on Rush.

461. Rush has been unjustly enriched at the expense of the Plaintiffs and Class members.

COUNT XI.
VIOLATION OF THE ILLINOIS EAVESDROPPING STATUTE
720 ILCS § 5/14-1, *et seq*.
<u>On Behalf of Plaintiffs and the Class</u>

462. The Illinois Eavesdropping Statute ("IES"), 720 ILCS § 5/14-1, *et seq*., prohibits the surreptitious interception, recording, or transcription of private electronic communications without the consent of all parties to the conversation and provides a civil cause of action to a person subjected to a violation of the IES against eavesdroppers and their principals.

463. Under 720 ILCS § 5/14-2(a)(3), the IES makes it unlawful for a person to knowingly and intentionally intercept, record, or transcribe, in a surreptitious manner, any private electronic communication to which he or she is not a party unless he or she does so with the consent of all parties to the private electronic communication.

464. Under 720 ILCS § 5/14-2(a)(5), the IES makes it unlawful for a person to knowingly and intentionally use or disclose any information which he or she knows or reasonably

should know was obtained from a private conversation or private electronic communication in violation of the IES, unless he or she does so with the consent of all of the parties.

465. Under 720 ILCS § 5/14-2(a)(4), the IES makes it unlawful for a person to knowingly and intentionally "possesses any electronic, mechanical, eavesdropping, or other device knowing that or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious overhearing, transmitting, or recording of private conversations or the interception, or transcription of private electronic communications and the intended or actual use of the device is contrary to the provisions of" the IES.

466. The IES defines "private electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation." 720 ILCS § 5/14-1(e).

467. "Surreptitious," as used in the IES, "means obtained or made by stealth or deception, or executed through secrecy or concealment." 720 ILCS § 5/14-1(g).

468. An "eavesdropper" means "any person…who operates or participates in the operation of any eavesdropping device contrary to the provisions of [the IES] or who acts as a principal[.]" 720 ILCS § 5/14-1(b).

469. A "principal" includes any person who "[k]owingly derives any benefit or information from the illegal use of an eavesdropping device by another" or "[d]irects another to use an eavesdropping device illegally on his or her behalf." 720 ILCS § 5/14-1(c).

470. An "eavesdropping device" is "any device capable of being used to…intercept…electronic communications[.]" 720 ILCS § 5/14-1(a).

471. Plaintiffs' communications with Rush constituted private electronic communications. Plaintiffs transmitted their communications to Rush from their computers or by wire, intended the communications to be private, and reasonably expected the communications to be private under HIPAA, Rush's express promises of confidentiality, the physician-patient relationship, and other State and federal laws protecting the confidentiality of Plaintiffs' communications.

472. Facebook, Google, and Bidtellect were not parties to Plaintiffs' private electronic communications with Rush. Plaintiffs believed they were only communicating with Rush, intended for their communications to be directed at Rush only, and were unaware of the presence of concealed source code that redirected their communications.

473. Facebook, Google, and Bidtellect's interceptions of Plaintiffs' private electronic communications were knowing, intentional, and surreptitious. Facebook, Google, and Bidtellect intentionally designed their source code so that it could be concealed on websites to secretly intercept private communications. On information and belief, Facebook, Google, and Bidtellect knew that their source code was capable of, and in fact did, intercept private electronic communications without the consent of all parties to the communications.

474. Facebook, Google, and Bidtellect used and disclosed Plaintiffs' intercepted communications for advertising purposes.

475. Facebook, Google, and Bidtellect's conduct was done without Plaintiffs' consent, in violation of 720 ILCS § 5/14-2(a)(3) and (a)(5).

476. Rush acted as Facebook, Google, and Bidtellect's "principal" under the IES. By deploying the source code from Facebook, Google, and Bidtellect on its web-properties, Rush directed that Facebook, Google, and Bidtellect illegally eavesdrop on Plaintiffs' private electronic

communications on its behalf and Rush knowingly derived benefits and information from the illegal eavesdropping in the form of marketing.

477. Rush further violated 720 ILCS § 5/14-2(a)(4) by possessing the source code, knowing that its design rendered it primarily useful for surreptitiously intercepting private electronic communications contrary to the IES.

478. Rush's violation of the IES was wanton, reckless, and/or malicious.

479. For Rush's violations of the IES, Plaintiffs and Class members seek actual damages, punitive damages, injunctive relief, and any other relief the Court deems just.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class members, respectfully requests relief against Rush as set forth below:

a. Entry of an order certifying the proposed Class and Class pursuant to Federal Rule of Civil Procedure 23;

b. Entry of an order appointing Plaintiffs as representatives of the Class;

c. Entry of an order appointing Plaintiffs' counsel as Class Counsel for the Class;

d. Entry of an order for injunctive and declaratory relief as described herein, including but not limited to:

i. Enjoining Rush, its affiliates, associates, officers, employees and agents from transmitting or disclosing Plaintiffs' and Class members' personally identifiable patient data and the contents of their communications to unauthorized third parties;

ii. Enjoining Rush, its affiliates, associates, officers, employees and agents from taking Plaintiffs' and Class members' personally identifiable patient data and the contents of their communications, and any other data except that for which appropriate notice and consent is provided;

iii. Mandating that Rush, its affiliates, associates, officers, employees and agents hire third-party monitors for a period of at least three years to ensure that all the above steps have been taken; and

iv. Mandating that Rush, its affiliates, associates, officers, employees and agents provide written verifications on a quarterly basis to the court and counsel for the Plaintiffs in the form of a declaration under oath that the above steps have been satisfied.

e. Enter judgment in favor of Plaintiffs and each of the other Class members for damages suffered as a result of Rush's conduct alleged herein, including compensatory, statutory, and punitive damages; as well as equitable relief including restitution and disgorgement, to include interest and prejudgment interest;

f. Award Plaintiffs their reasonable attorneys' fees and costs; and

g. Grant such other and further legal and equitable relief as the court deems just and equitable.

JURY DEMAND

Plaintiffs demand a trial by jury on all claims so triable.

Dated: April 11, 2023

Respectfully Submitted,

/s/ Corban S. Rhodes
DICELLO LEVITT LLC
Adam J. Levitt
Amy E. Keller
Nada Djordjevic

Sharon Cruz
Ten North Dearborn St., Sixth Floor
Chicago, Illinois 60602
Tel.: (312) 214-7900
Fax.: (312) 253-1443
alevitt@dicellolevitt.com
akeller@dicellolevitt.com
ndjordjevic@dicellolevitt.com
scruz@dicellolevitt.com

DICELLO LEVITT LLC
David A. Straite*
Corban Rhodes*
485 Lexington Ave., 10th Floor
New York, NY 10017
Tel.: (646) 933-1000
Fax.: (646) 494-9648
dstraite@dicellolevitt.com
crhodes@dicellolevitt.com

SIMMONS HANLY CONROY LLC
Jason 'Jay' Barnes*
112 Madison Ave., 7th Floor
New York, NY 10016
Tel.: (212) 784-6400
Fax: (212) 213-5949
jaybarnes@simmonsfirm.com

Attorneys for Plaintiffs

**Pro hac vice*